virus BULLETIN Covering the global threat landscape

MWI-5: OPERATION HAWKEYE

Gabor Szappanos
Sophos, Hungary

While *Microsoft Office* malware is no longer as prevalent as it was in the 1990s, it retains a notable presence. In place of the previously dominant macro viruses, nowadays we see downloader and dropper trojans that are used in spear-phishing and targeted email attacks. In these efforts the criminals rely on malware generators.

The most influential *Office* malware creation kit today is Microsoft Word Intruder (MWI), developed in Russia.

Despite its influence, MWI was unknown to the general public until *FireEye* released a blog entry describing it early in 2015 [1]. Shortly after that, further reports surfaced [2–5]. However, these reports turned out just to be the tip of the iceberg.

Attacks launched with the help of MWI are usually deliberately kept small. Some cybercrime groups appear to be changing their tactics: instead of aiming to infect hundreds of thousands of computers they infect a few thousand or even just a few dozen victims at a time. This approach helps them to stay under the radar and avoid unwanted attention.

In a recent piece of research we mapped out a wide variety of MWI attacks that took place between May and August 2015 [6]. The research paper provides detailed information about the internals of MWI and the additional server-side module, MWISTAT. In this article we will assume that the reader is already familiar with those details.

We followed at least a dozen different cybercrime groups that have used the MWI malware generator to deploy more than 40 different malware families.

In this article we detail one particular distribution operation, during which a commercial keylogger application was distributed in large parts of Asia.

INFECTION VECTOR

The infection campaigns were observed from the middle of March 2015 and lasted until the end of July 2015, using two different MWISTAT servers. After this period we observed no further activity.

The primary infection vector used in this operation consisted of spear-phishing email messages with exploited Rich Text Format (RTF) documents as attachments. The documents were generated with Microsoft Word Intruder.

The email messages used the theme of purchase requests from India to Vietnam, which correlates well with the regional focus of the operation – as we will see later, these two countries were among the main targets.

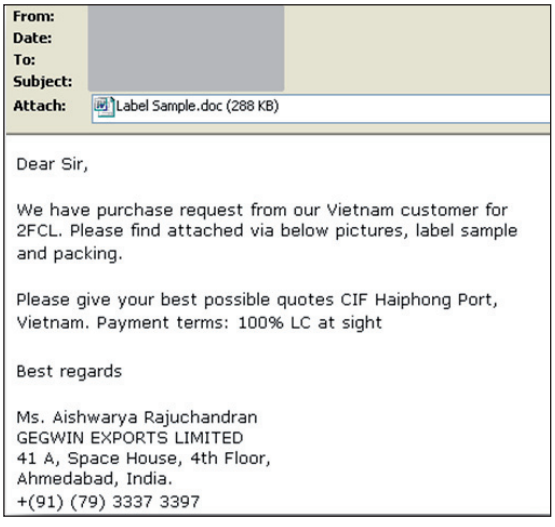

Figure 1: The email messages used the theme of purchase requests.

Later on, after the first C&C server was shut down, the criminals switched to a new server. In this period we observed a different phishing theme, featuring a bank transaction receipt.

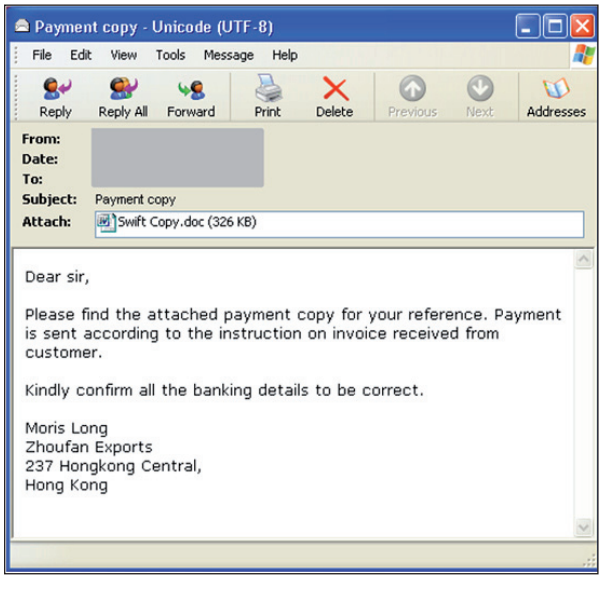

Figure 2: A different phishing theme was observed, featuring a bank transaction receipt.

First seen	Original name	SHA1
13/03/2015	Vietnam order.doc	bec0dbb5bd468da8f92a038d547f8e3e3bfef828
27/05/2015	Plans and Designs.doc	80ac4199c7c519cbbcc04087a684b776cfe2b24a
29/05/2015	Invoice.doc	4aa4e3d70a5af774d95db2a1926fc2c455072f73
08/06/2015		8b628278c6b032b26ac5cac84abbdb1ab0777668
08/06/2015	Payment Copy.doc	2894a0e6bf28e18cf820064dc1ad12d0fee05052
09/06/2015		e9e294e6cfaf064373e4600319657f69e2bed278
11/06/2015	Label Sample.doc	8afd513d177f99fe4ef95ba5a26c009f9e48b637
11/06/2015	Original BL	b724a030ef3d3ca5aacba76c11bbeb72193f7558
11/06/2015		27f59ac9b5796b46bb13cf9dc85bb5e8893a96d5
12/06/2015	Remodel+plan.doc	bbb7e5d092f7e4a56cf0be51d1c586c61f63f44d
15/06/2015	Shipping Doc.doc	bb33f094b2f9c940b25518efcb9eb1dc38612be8
28/07/2015	Payment copy.eml	9aa2372ebaac689c503a07a693a305aa845539b2
28/07/2015	PO_Vietnam Order.doc	05468cb85b2ef4f63ffc2256414eb984315e7600
28/07/2015		c17f283852e9054c5a99fab2ced81dcdb7717ae0
28/07/2015		5cc410e31e5e84e980039e99cae47cbabae85a5c

Table 1: A handful of the documents used by the group over time.

We found a handful of different documents used by the group as email attachments over time, as shown in Table 1.

The original name of the attachments suggests that most distribution campaigns used one of the two previously mentioned themes (shipping labels or payment receipts).

DISTRIBUTED PAYLOAD

All of the exploited document samples were downloaders that installed the HawkEye password stealer program.

Figure 3: The HawkEye keylogger was installed and immediately started to gather user credentials.

When the attached document was opened, the payload was downloaded and executed; this installed the HawkEye keylogger, which immediately started to gather user credentials (Figure 3). HawkEye is a commercial keylogger tool [7] that logs keystrokes and clipboard content, and can gather all imaginable passwords.

The product supports email or web upload for the stolen information, but in the scope of this operation the FTP drop

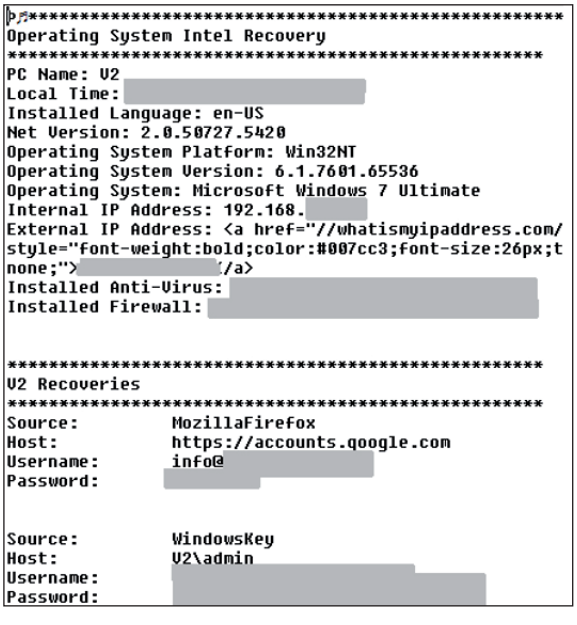

Figure 4: The capture files are plaintext with content similar to this.

method was the most commonly used. However, there is evidence that at some point the criminals also tried email submission.

The stolen information was uploaded at regular intervals to the server. The capture files are plaintext with content similar to that shown in Figure 4.

HawkEye seems to be a popular choice in crimeware operations: recent encounters have been documented in [8] and [9]. Further evidence indicates that MWI-5 was very likely operated by the criminal group identified in the *Trend Micro* report.

SERVER ARCHITECTURE

Over the duration of the operation the following servers were used as MWISTAT C&C servers:

six-bro.com

amittrade.com

Six-bro.com was the server that was most actively used during the campaigns. Our data indicates that operations related to this server began in mid-March, and finished at the end of June 2015, when the server was shut down.

During the server's active period, multiple installation directories were observed, with MWISTAT apparently installed under three different subdirectories: webstat, webbie and wbst (see Table 2).

This is not unusual; the same behaviour was observed by *Check Point* researchers [10], in their case with seven different install locations. The reason could be the same in both cases: upgrade of the MWISTAT software to a new version. The criminals probably didn't want to overwrite the already up and running installation with the new release, and instead created a new installation directory, and the new campaigns started to use the new version.

While the six-bro.com server was active, another domain, labelcounty.com, pointed to the same IP address. That alone would not indicate a connection; six-bro.com was hosted on namecheap.com, using shared IP addresses – dozens of domains pointed to the same IP address. However, the web server itself contained a subdirectory (www.six-bro.com/labelcounty.com) with the content shown in Figure 5.

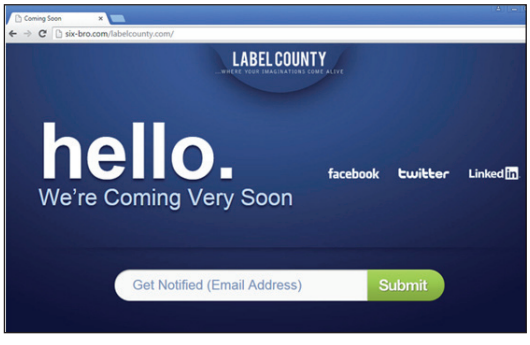

Figure 5: Content of the subdirectory www.six-bro.com/labelcounty.com.

At the time of writing this article, the primary C&C domain has been shut down, labelcounty.com has been moved to a

2015-06-12	http://six-bro.com/**webstat**/img.php?id=70998668
2015-06-12	http://six-bro.com/**webstat**/img.php?id=33816634
2015-06-12	http://six-bro.com/**webstat**/img.php?id=23900374
2015-06-11	http://six-bro.com/**webstat**/img.php?id=12464729
2015-06-11	http://six-bro.com/**webstat**/img.php?id=38915948
2015-06-09	http://six-bro.com/**webstat**/img.php?id=55731239
2015-06-08	http://six-bro.com/**webstat**/img.php?id=82357659
2015-06-08	http://six-bro.com/**webstat**/img.php?id=88290212
2015-05-29	http://six-bro.com/**webstat**/img.php?id=50981746
2015-04-22	http://six-bro.com/**webbie**/img.php?id=90222451
2015-04-20	http://six-bro.com/**webbie**/img.php?id=84085197
2015-04-20	http://six-bro.com/**webbie**/img.php?id=95536720
2015-03-20	http://six-bro.com/**wbst**/image.php?id=88321021
2015-03-17	http://six-bro.com/**wbst**/image.php?id=89864851
2015-03-17	http://six-bro.com/**wbst**/image.php?id=40074095
2015-03-13	http://six-bro.com/**webstat**/image.php?id=35878151

Table 2: MWISTAT was apparently installed under three different subdirectories: webstat, webbie and wbst.

different location, but the content is still the same 'under-construction' page. There is no track record for this server, either for malicious or benevolent use of it. It is likely that the criminals are keeping it for a future opportunity.

The six-bro.com domain was shut down in the middle of July 2015. This was not a hacked domain; it was registered and maintained by the criminals. By the end of that month the operation had been transferred to the second C&C domain, amittrade.com, also maintained by the criminals, where it ran until the end of July. The last sample related to this operation was observed on 28 July 2015.

The overall purpose of the operation is not absolutely clear, but we can make educated guesses. HawkEye is capable of stealing a very wide range of credentials, along with keylogs and clipboard data. There are many possible uses for the stolen data, ranging from industrial espionage to identity theft. However, there is some indication that in this case the attackers were interested in banking credentials.

The six-bro.com domain contained another interesting subpage, which was a fully featured online banking page, perfectly suited for phishing attacks (Figure 6).

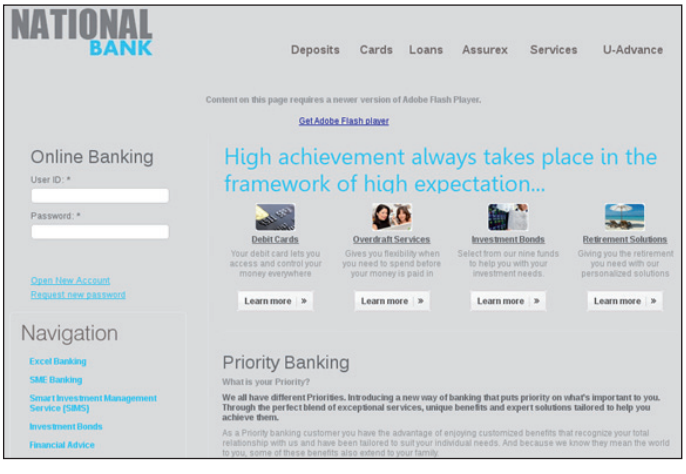

Figure 6: A fully featured online banking page on a subpage of the six-bro.com domain.

Coincidentally, six-bro.com was reported as a fake banking site [11] with the same National Bank theme. It seems that the criminals tried to reuse components from an earlier banking scam site, nb-national.com [12], dating back to 2012, indicating prior interest in banking fraud. However, in this case, it is more likely that they were interested in using the stolen credentials to access corporate webmails, to gather information and use it in more targeted change of supplier fraud.

CAMPAIGN STATS

The malicious documents contain the MWISTAT callback address in the following form:

```
INCLUDEPICTURE "http://{serverpath}/
{mainscript}?id={campaign_ID}
```

During this operation two different servers were used, and on the first server three different installations. Overall, we have seen 10 different campaign IDs, suggesting that at least 10 distribution campaigns were executed by the criminals.

The number of victims of the individual campaigns ranged widely between a few dozen and a few thousand. This is a low number compared to the reported number of ransomware or Zbot victims, but the terms and conditions of MWI do not permit larger campaigns. Nevertheless, it produces a solid income for the criminals.

The largest campaigns focused on the continents of Asia and Africa, the most affected countries being Indonesia, India, Thailand, Oman and Malaysia.

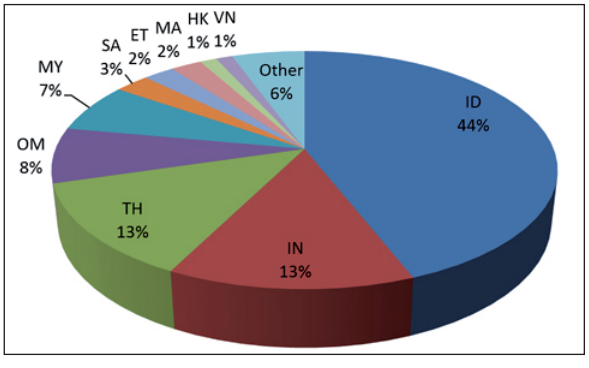

Figure 7: The most affected countries were Indonesia, India, Thailand, Oman and Malaysia.

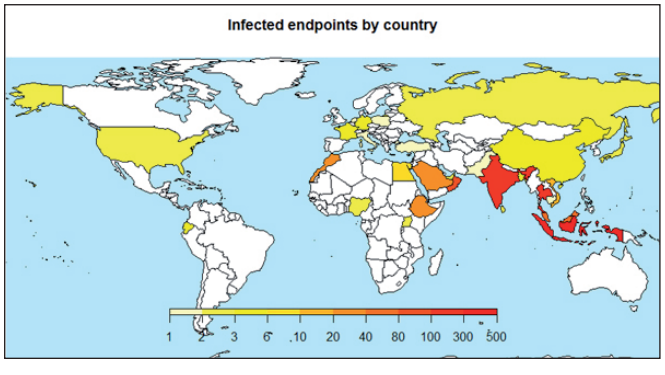

Figure 8: Map of infected endpoints.

SUMMARY

It is reasonable to assume that this MWI-related campaign is aimed at gathering user credentials, especially corporate webmail accounts.

The group behind the attack used email messages to reach their targets, with Rich Text Format documents as attachments.

These documents exploited three different vulnerabilities: CVE-2012-0158, CVE-2013-3906 and CVE-2014-1761. Even CVE-2014-1761, the latest of the vulnerabilities, had been patched about a year before these attacks started.

It shouldn't be difficult to protect against the activities of this group: simply applying the relevant patches for *Microsoft Office* should disarm the attack. Then there is only one remaining piece of advice: don't fall for social engineering.

REFERENCES

[1] https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html.

[2] http://blog.checkpoint.com/2015/06/26/microsoft-word-intruder-rtf-sample-analysis/.

[3] http://blog.0x3a.com/post/117760824504/analysis-of-a-microsoft-word-intruder-sample.

[4] https://www.proofpoint.com/threat-insight/post/Foot-in-the-Door.

[5] http://www.welivesecurity.com/2015/04/09/operation-buhtrap/.

[6] https://blogs.sophos.com/2015/09/02/microsoft-word-intruder-revealed-new-sophoslabs-research-goes-inside-a-malware-creation-kit/.

[7] http://hawkeyeproducts.com/.

[8] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hawkeye-nigerian-cybercriminals-used-simple-keylogger-to-prey-on-smbs.

[9] http://www.isightpartners.com/2015/06/hawkeye-keylogger-campaigns-affect-multiple-industries/.

[10] http://blog.checkpoint.com/2015/06/26/microsoft-word-intruder-rtf-sample-analysis/.

[11] http://db.aa419.org/fakebanksview.php?key=94793.

[12] http://www.malwareurl.com/ns_listing.php?ip=176.8.205.173.

Editor: Martijn Grooten

Chief of Operations: John Hawes

Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca, Lewis Jones, Ionuţ Răileanu

Sales Executive: Allison Sketchley

Editorial Assistant: Helen Martin

Developer: Lian Sebe

Consultant Technical Editor: Dr Morton Swimmer

© 2015 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England

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

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