A Comprehensive Analysis on Bamital Botnet

Yogesh Anandhakumar
MSc Cyber Security
National College of Ireland
Dublin, Ireland

***Abstract*—The Bamital is a malware family, mainly used in clickfraud and search hijacking activities, which makes it a dangerous threat in the field of cybersecurity. The Bamital can be tracked from 2009 and finally shut down by Symantec & Microsoft in 2013. This paper discusses a comprehensive analysis of Bamital botnet, looking at its size, behavior, architecture, operation, impact, etc., and mitigations. This analysis is provided by conducting an extensive review of the existing literature, and industry reports. The research also addresses the overview of the available detection techniques and how these affect the security procedures. This analysis presents the scope of Bamital's operations, which have impacted millions of IP addresses worldwide and produced estimated revenues exceeding $1 million annually for its operators. This research shows the necessity of continuous modification in cybersecurity tactics to tackle the obstacles presented by Bamital and similar cyber threats.**

Keywords—Bamital, Botnet, Bot, Malware, Trojan, click fraud.

I. Executive Summary

Bamital's origin can be traced back to late 2009, which is successfully shutdown on Feb 06, 2013 by Symantec and Microsoft.

https://de.wikipedia.org/wiki/Bamital

Click fraud or Clickjacking is a type of fraudulent activity, which tricks users to click on the link or advertisement, which leads the user to a specific website which is controlled by the attacker, where the user is not intended to visit. The Bamital is a malware family, which is mainly used in clickfraud and search engine hijacks. The purpose of the clickfraud is to generate income by increasing the number of clicks on Ad or Link, or increasing web traffic of a specific website by triggering users to click on ads or links, and redirecting them to a C&C server which is hosting the ads of the attacker.

https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=e0cdc179-449d-4b4a-9104-6a98890c4e9d&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

https://docs.broadcom.com/doc/intelligence-report-jan-13-en

This analysis is done by a comprehensive literature review of research papers, industry reports, conferences, etc. The main objective of this analysis is to analyze and understand how the Bamital botnet, a dangerous windows based botnet, is utilized in generating revenue for the attackers by involving users or victims to clickfraud and search hijacking activities. Furthermore, without any input from the user, Bamital creates network traffic that is not initiated by the user, such as website visits and ad clicks. Over 1.8 million distinct IP addresses were found to be interacting with a single Bamital command-and-control (C&C) server during a six-week period in 2011. Additionally, an average of three million clicks were being hijacked every day. Click-jacking and the redirection have exposed users to more malware, including spyware disguised as antivirus software. The history of Bamital can be traced back to late 2009, and during the past couple of years, it has seen several changes. Drive-by-downloads and malicious files on peer-to-peer (P2P) networks have been the main methods of infection utilized by Bamital. When Symantec was allowed to collaborate with Catalunya CERT (CESICAT) and Spain's Civil Guardia to examine a Spanish-hosted instance of the botnet's C&C server, the study and investigation into Bamital picked up speed in late 2011. The attackers revenue is roughly estimated to be $1.1 million a year based on information found on this server.

https://docs.broadcom.com/doc/trojan-bamital-13-en

Online vendors typically aim to boost sales through search engine results placement, placement of adverts on pertinent websites, and increased exposure and traffic. The aim of clickfraud is to increase click-through rates on advertisements or traffic (network traffic) to a particular website to make money. In the first case, suppliers pay the ad-distribution networks according to the frequency with which end users click and follow advertisements on websites, so assuming the role of marketers. The responsibility for posting the advertisement on websites that seem relevant to the advertiser's content, falls on the ad-distributor. Ad-distributors and advertisers are most familiar with pay-per-view (PPV) and pay-per-click (PPC) payment methods. With pay-per-click (PPV) advertising, the ad-distributor receives payment for simply placing the advertisement on websites, regardless of whether the user clicks through or not. But under the PPC arrangement, the advertiser only pays the distributor when a customer clicks on the advertisement and goes to the vendor's website. These two methods of delivering advertisements are still leading to fraud.

https://docs.broadcom.com/doc/trojan-bamital-13-en

II. Methodology

A. *Literature review*

This analysis has been done by a comprehensive literature review of research papers, industry reports, online malware databases. The literature review is carried out to gather details like behavior, architecture, operations, impact and mitigations of the Bamital botnet. A detailed document about Bamital botnet has been published by Symantec. This document gave a complete understanding of the Bamital botnet. Also few reports and documents from Microsoft, Krebson Security, GeekWire, Dark Reading, Hybrid analysis, Virus Total, etc., gave a very brief understanding about the Bamital botnet and its effects.

B. *Working of Trojan.Bamital*

The below explains the working of Bamital Botnet.

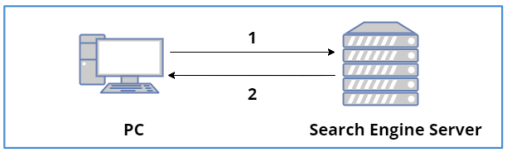

Fig. 1. Uninfected machine behavior

The above image represents the clean system and its behavior.

- Step 1: User requests something from a clean system, the browser connects to the search engine server.
- Step 2: The search engine server will sends the search results of the user's request to the user's computer. Then if the user clicks on a result brings them to the intended website.

https://www.youtube.com/watch?v=4nnV4KeWQj0

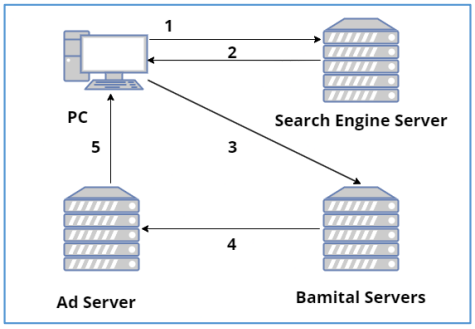

Fig. 2. Infected machine behavior

The above image represents the Bamital botnet affected system's behavior.

- Step 1: User requests something to the search engine server, with a Bamital infected system. The browser connects to the search engine server
- Step 2: The search engine server will sends back the results to the user's computer.
- Step 3: If the user clicks on any of the results from the search engine server, they will be redirected to the Bamital servers.
- Step 4: Then the Bamital servers will then connect with the Ad server.
- Step 5: This brings the results from the ad server to the user's computer. If the user clicks any results, those results will take the user to unintended websites.

If the Bamital servers cannot serve customized websites, tainted search results will be returned to the user's browser instead. Those results will lead to fake websites.

https://www.youtube.com/watch?v=4nnV4KWQj0

C. *Data Collection:*

As the Trojan.Bamital gets into a system when a user visits a website that is owned or controlled by attackers, where the users will be directed to other pages which contains the malicious software packages. This is how Trojan.Bamital enters into the systems.

Now we have got few details about the Trojan.Bamital in many industry reports and malware databases.

D. *Data Analysis:*

Then I analyzed the hashes from those reports and databases, in Hybrid analysis and Virus total. The results are below,

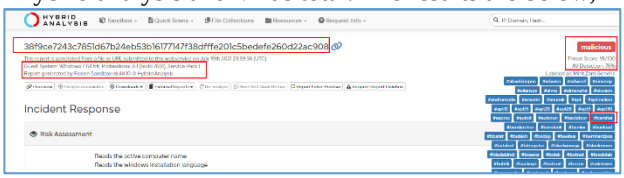

Fig. 3. Hash Analysis in Hybrid analysis.

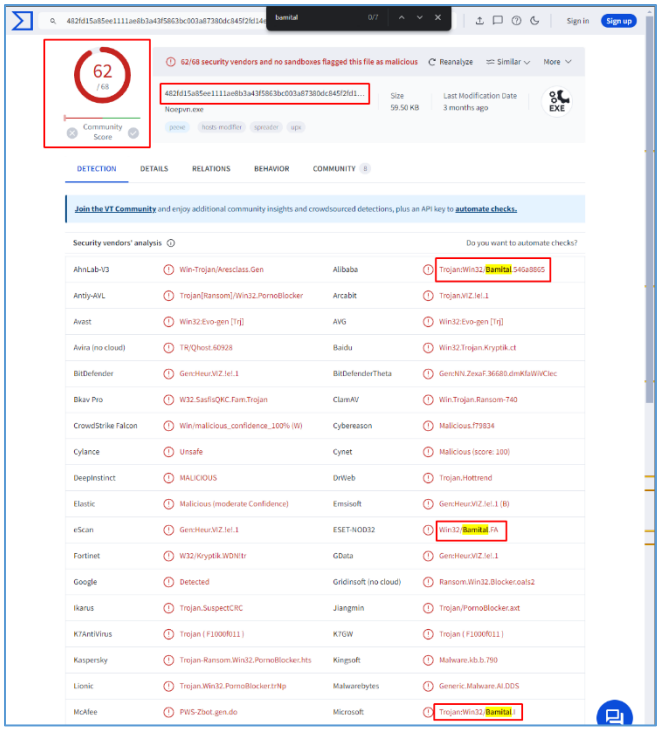

Fig. 4. Hash analysis in Virus Total

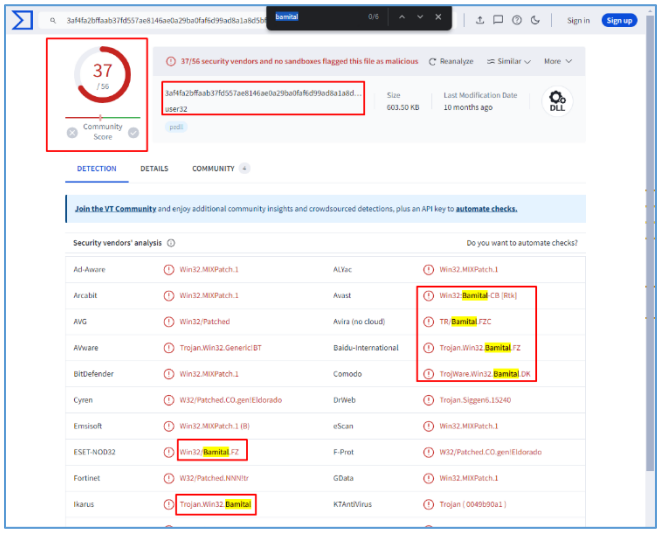

Fig. 5. Hash analysis in Virus Total

Bamital targets the below mentioned strategies in two distinct ways when committing click fraud.

Initially, Bamital takes over all clicks on specifically targeted search engine result pages, including links and ads, and redirects them to an attacker-controlled C&C server that has been predetermined. To determine where the user should

be redirected, the C&C server uses information about the search query (keywords) and the address of the website that the original search engine intended to lead the user. For instance, if the end user searched for antivirus and the search engine intended to send the user to a Symantec owned page. The attacker-controlled server would use this information in its decision logic to redirect the user's compromised computer to a third-party website that uses the Symantec brand name and sells bogus antivirus programs. In this way, the operators of Bamital take on the role of ad networks and get payment from the advertisers (false antivirus vendors).

Secondly, Trojan.Bamital interacts with its C&C server and browses several websites within a browser instance, mimicking the actions of an actual user. Bamital mimics queries made with certain keywords on search engines under the control of attackers. When Bamital receives responses from these attacker-controlled servers that appear to be search engine results, it uses the self-initiated browser instance to visit the website. Because this technique operates in the background, computer users may not even be aware of the network activity while using it, nor do they see the browser window that is being used. By using this procedure, Bamital operators can act as traffic brokers, creating and selling traffic from bogus consumers to any vendor they choose.

III. Botnet Investigation And Findings

A. *Bots Identification*

- A family of malware known as Win32/Bamital alters the host files to capture browser traffic and block access to specific websites related to security. It is possible for Bamital versions to alter some authentic Windows files to carry out their payload. The Bamital family has been utilized to do click-fraud in nature. This Trojan enters a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.
- "How did I get infected with Bamital?
- A system can be infected with this malware when a user visits a website that is owned by attackers. The user is diverted to other pages that contain malicious software packages; these packages are responsible for installing Bamital."

https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Bamital/Bamital.html

- Name of Malware: Bamital (Sheedash, Lavandos)
- File type: Executable (Windows PE file)
- Memory resident: No

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TROJ_BAMITAL.WC/

- Hashes:

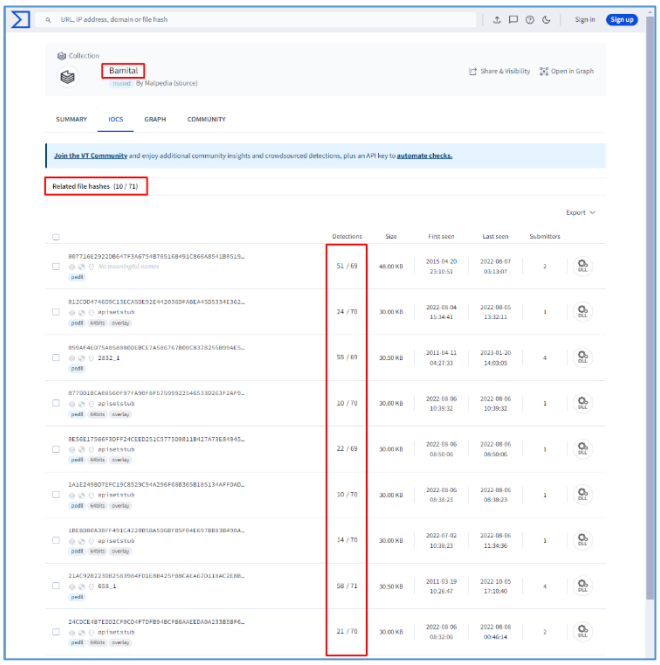

Fig. 6. Hashes

Detection by few AV's:

- Symantec=Trojan.Bamital and Trojan.Bamital.B
- Microsoft=Win32/Bamital,TrojanDropper:Win32/Bamital.A,Trojan:Win32/Bamital.E, etc.
- Avast = win32:Bamital-X
- TrendMicro = TROJ_BAMITAL.WC

B. *Botnet Size and Damage*

- Type of Malware: Click fraud.
- Impact: high
- Size: varies
- In few reports of TrendMicro, the sizes of Bamital trojan are TROJ_BAMITAL.WC = 62,976 bytes, TROJ_BAMITAL.SMH = 49,152 bytes, TROJ_BAMITAL.SMD = 38,400 bytes, PE_BAMITAL.SA-O = 63,488 bytes.
- While monitoring a single Trojan.Bamital C&C server over a 6-week period in 2011, over 1.8 million IP addresses communicating with the server and an average of three million clicks been hijacked daily, and the attacker revenue was around $1.1M annually.

C. *Target Devices*

- Affected Device Types: PCs, laptops.
- Affected Operating Systems: Windows
- Affected applications: Browsers like Google chrome, Firefox, Yahoo, etc.
- Drive-by-downloads and malicious files on peer-to-peer (P2P) networks have been the main methods of infection utilized by Bamital trojan.

D. *Botnet Architecture*

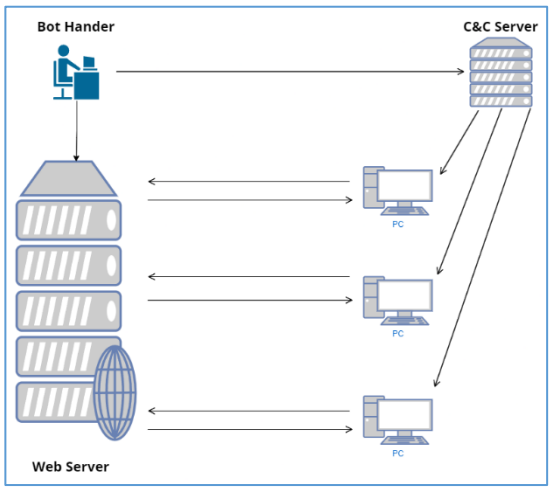

Fig. 7. Architecture

As shown in the above figure, the normal users will be visiting to the malicious sites, handled by the bot handler. Once they click on the link or ad in the malicious website, then the trojan gets downloaded and changes happened in the browser as well registry. This is how the Bot Handler of Bamital trojan infects and takes control of the victims machines.

E. *Botnet Behavior*

- The Bamital trojan uses distribution methods like Drive-by-downloads and malicious files on peer-to-peer (P2P) networks.
- Once the dropper gets downloaded, the malware will be installed and executed, also changes the windows registry files, AutoStart apps, etc.
- Then the infected machines connect to the C&C server and receive instructions, updates, and reports back the status of machine.
- It uses the HTTP, IRC or P2P protocols for communications.
- The Bamital botnet's main purpose was search engine hijacks & clickfraud, so after infection, the infected machine or bots, they will generate revenue for the attacker, by clicking on ads or links in the background.

F. *Botnet Resilience*

- The core module of Bamital trojan does not have a static domain, it uses a dynamic domain generation algorithm(DGA) to give domain name for the C&C server. This module gets the current date by sending a request to google. Then the DGA uses the date as seed and ends with .in, .info, .co.cc to create a total of 15 pseudorandom server names per day for the C&C server. Then it tries to find out which of these 15 domains has the required data by contacting all the 15 servers.
- During a two week period of July 2012, in one specific case, the attackers used the below mentioned domains,
    - 7/10/12 - jytajigefynizer.info
    - 7/11/12 - kevikoneculunyw.info
    - 7/12/12 - zesedywokedapef.info
    - 7/13/12 - xidotuhobaxuxah.info
    - 7/14/12 - tizemeginuxutuc.info
    - 7/15/12 - zyfesiwejotijar.info
    - 7/16/12 - coviqujucybimob.info
    - 7/17/12 - kupecyxakegyzan.info
    - 7/18/12 - gedowaqoqyniqos.info
    - 7/19/12 - xamixiwetomegum.info
    - 7/20/12 - suhewyhacagalaj.info
    - 7/21/12 - joqutuxogenecen.info
    - 7/22/12 - dobihebogocupiw.info
    - 7/23/12 - vefefuqijalecit.info
- For persisting in the infected machines, the trojan modifies the windows registry files and AutoStart entries to ensure persistence even after reboot.

G. *Botnet Takedown*

- When Symantec was allowed to collaborate with Catalunya CERT (CESICAT) and Spain's Civil Guardia to examine a Spanish-hosted instance of the botnet's C&C server, the study and investigation into Bamital picked up speed in late 2011. The attackers revenue is roughly estimated to be $1.1 million a year based on information found on this server. During February 2013, Microsoft and Symantec collaborated to takedown the Bamital botnet.

H. *Botnet Evolution*

Define abbreviations

IV. Recommendations

Before you begin

V. Conclusions

Before you begin

VI. References

Before you begin

VII. Appendix

Before you begin

A. Units

- Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as “3.5-inch disk drive”.
- Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- Do not mix complete spellings and abbreviations of units: “Wb/m2” or “webers per square meter”, not “webers/m2”. Spell out units when they appear in text: “. . . a few henries”, not “. . . a few H”.
- Use a zero before decimal points: “0.25”, not “.25”. Use “cm3”, not “cc”. (*bullet list*)

B. Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

$$a + b = \gamma \tag{1}$$

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use “(1)”, not “Eq. (1)” or “equation (1)”, except at the beginning of a sentence: “Equation (1) is . . .”

C. Some Common Mistakes

- The word “data” is plural, not singular.
- The subscript for the permeability of vacuum μ_0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter “o”.
- In American English, commas, semicolons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
- A graph within a graph is an “inset”, not an “insert”. The word alternatively is preferred to the word “alternately” (unless you really mean something that alternates).
- Do not use the word “essentially” to mean “approximately” or “effectively”.
- In your paper title, if the words “that uses” can accurately replace the word “using”, capitalize the “u”; if not, keep using lower-cased.
- Be aware of the different meanings of the homophones “affect” and “effect”, “complement” and “compliment”, “discreet” and “discrete”, “principal” and “principle”.
- Do not confuse “imply” and “infer”.
- The prefix “non” is not a word; it should be joined to the word it modifies, usually without a hyphen.
- There is no period after the “et” in the Latin abbreviation “et al.”.
- The abbreviation “i.e.” means “that is”, and the abbreviation “e.g.” means “for example”.

An excellent style manual for science writers is [7].

VIII. Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

A. Authors and Affiliations

The template is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

1) For papers with more than six authors: Add author names horizontally, moving to a third row if needed for more than 8 authors.

2) For papers with less than six authors: To change the default, adjust the template as follows.

a) Selection: Highlight all author and affiliation lines.

b) Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select the correct number of columns from the selection palette.

c) Deletion: Delete the author and affiliation lines for the extra authors.

B. *Identify the Headings*

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is "Heading 5". Use "figure caption" for your Figure captions, and "table head" for your table title. Run-in heads, such as "Abstract", will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named "Heading 1", "Heading 2", "Heading 3", and "Heading 4" are prescribed.

C. *Figures and Tables*

a) Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence.

TABLE I. TABLE TYPE STYLES

Table Head	**Table Column Head**		
	Table column subhead	***Subhead***	***Subhead***
copy	More table copy[a]		

[a] Sample of a Table footnote. (*Table footnote*)

Fig. 8. Example of a figure caption. (*figure caption*)

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity "Magnetization", or "Magnetization, M", not just "M". If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write "Magnetization (A/m)" or "Magnetization {A[m(1)]}", not just "A/m". Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

ACKNOWLEDGMENT *(Heading 5)*

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression "one of us (R. B. G.) thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi TIFF or EPS file, with all fonts embedded) because, in an MSW document, this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on your frame, use the MSWord "Format" pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.

REFERENCES

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] was the first ..."

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.