# Boutique Malware – Custom made attacks on e-business

Jonathan Juin Yang Pan and Chun Che Fung

*School of Information Technology, Murdoch University, Perth, WA*

Jonathan.Pan.JY@gmail.com l.fung@murdoch.edu.au

*Abstract*—**Malware are typically known through extensive publicity in the media when incidents such as infection by Conficker on the computers around the globe. Such Malware infects all who are vulnerable to its bite. However there is another form of Malware lurking which is not reported in any media, nor does it attack everybody. It targets only specific individuals and organizations. This form of Malware is seeking to achieve focused objectives rather than to drawing fame onto itself. The Malware is able to circumvent even the best practices used in security defences. Anti-Malware solutions are available but can be ineffective against them. The development approach to such Malware has evolved towards a bespoke development. Investigators and analysts of Malware face a great challenge in studying and combating against these Malware. This paper serves to expose such practices and to initiate discussions and strategies in order to develop counter-measure solutions that are urgently needed in the world of e-Business before the community is totally succumbed by this type of Boutique Malware.**

## I. Introduction

Malware is becoming a major problem to the global computing community - from users around the world to astronauts in space. Most Malwares are used by cybercriminals to conduct their criminal activities. According to FBI, the global hacker's economy is worth more than USD 10 billion annually [1] and Malware is a key contributor to this economy. In order to manage this malice and its negative impacts, there are numerous defensive approaches that organizations would typically adopt in order to safeguard their IT assets. There are the anti-virus solutions, intrusion detection and prevention systems, and other forms of layered security measures. However, there is an arsenal from the cybercriminal community that seems to be giving them an advantage. Unlike notorious mass attacks induced by highly publicized Malwares, this new form of Malware is conducting discrete attacks on specific organizations or individuals. Their goal is to minimize publicity in order to achieve their malicious intent on specific target or targets. The trend towards using such targeted Malware is growing from year to year. It started notably in 2005, with a number of reported attacks made to government organizations [4]. In 2008, more targeted attacks were launched. An example is an attack made against Hannaford Bros [5], grocery stores in New England USA. Four million of their credit and debit card numbers were stolen by a Malware developed specifically for them and to circumvent their security measures. According to a research group, such targeted Malware attacks is becoming a norm now [32]. A new definition for such form of Malware is called Advanced Persistent Threat (or APT) which takes its root from the military sector [33]. This form of Malware is a notable change from the 'write-once-attack-all' approach that seeks to infect as many as possible towards a 'write-once-attack-one' approach of where damage caused from the cyber assault is focused. An analogy to conventional weaponry would be smart bombs over conventional bombs. In this paper, this form of Malware is termed as "*Boutique Malware*" as we are looking specifically into its focused attributes. In this survey paper, the notable characteristics are discussed in the next section. The subsequent section, Section III, will look into the effectiveness of the current countermeasures with recommendations proposed. This is then followed by the research advancement considerations and finally the conclusion.

## II. Boutique Malware

Boutique Malware has a number of unique characteristics when compared to conventional Malware. It has the following features:

a. Targeted strategy
b. Bespoke development approach
c. Narrowly focused approach to infect the targeted
d. Customized attack techniques used to suit environment

### *A. Targeted Strategy*

Today, records show that only amateur hackers are getting caught by the police [1]. Professional cybercriminals are using subtle approaches in their Malware infections and attacks. They are kept intentionally elusive to stay below the radar of the security and law enforcement communities. To stay totally evasive as long as possible is a key objective [2]. It would be a mission failure if the Malware gained fame and publicity. The Malware also is required to slip through cracks found in the multiple layers of defences to get to its target. Mission goals are typically financial gains or politically motivated objectives rather than fame.

Boutique Malware focuses on specific targets. They include government entities [18], schools [13], banks [7], military organizations [14], political entities, [15] corporate CEO [16] and other high salaried workers at selected corporations [17]. Such Malware also targets specific type of users that are associated with the targeted organization. An example is the customers doing online banking with specific bank or banks [19].

### B. *Bespoke Development Approach*

The design of such Malware is more elaborate compared to the common wild fire Malware. A customized based development approach is used to develop Boutique Malware. According to Horenbeeck [4], these tailored made Malware are developed in the following manner.

a. Identify the specific actors involved including the targeted.
b. Find logical associations between communities which the identified actors associate with often.
c. Gather information about the actor's reputation in the community, their interests and contact information through the activity they generate online.
d. Design and develop the Malware to infiltrate the actor's protected space and information store.
e. Send the uniquely developed Malware to the targeted and deceive the latter into installing the Malware.

Such sequence of activities is similar to the techniques used by hackers as part of their hacking cycle. The extensive amount of reconnaissance done on the targeted to identify vulnerabilities and operating patterns would incur more time and effort in the development of Boutique Malware design than the typical Malware [2]. Schouwenberg [6], who did a study into Boutique Malware that targeted banks, noted that such Malware are modifications or derivatives of a common species or past variants of Malware. They were custom designed to infect its targeted then manoeuvre around the bank's security defences. A group of researchers recently discovered a targeted Malware compromising of over 87,000 Malware variants [31]. Boutique Malware is creating a new form of business for Malware developers from creating Malware for the masses to bespoke Malware where the finished product is custom made to operate 'effectively' within the target's operating environment.

### C. *Narrowly Focused Infection Approach*

The infection vector used in such Malware is focused on specific persons or group of interest. Here the intent is to infiltrate the target's operating environment. However such targets would likely have a comprehensive set of defence measures in place to protect them. Boutique Malware are adapted to slip through the layers of defences. Targeted deceive techniques are used. For example, they use specific references to address their targets to deceive the targets. References like name, title and company name of the targeted are used. According to Germain [17], it seems unlikely that emails used in such malicious attack are automatically sent by software bots. Such targeted phishing attacks made by cybercriminals against specific individuals or entities are known as Spear-phishing. Such forms of social engineering attacks are not easily detectable [20]. Such assaults may result in the victim not being aware that a breach has even occurred as the activity may be deemed legitimate by the victim.

The key notable characteristics of specific infection strategy used include:

a. Specific references that uses knowledge of the personal information of a specific individual or organization [21].
b. The focus is on individuals or organizations within a specific region [7] with language localization made to the malicious communiqué sent to the targeted [13].
c. Timing on the execution of infection attempt is deliberately chosen. An example is malicious emails being sent on weekends instead of weekdays [18].
d. Specific infection tools or platform that best suits the targeted are used. For example, using Microsoft Office exploits with Microsoft Word and Microsoft Powerpoint documents [18].
e. Use of social engineering techniques to deceive the victim into thinking that the email is legitimate [17]. An example is to falsify the origins of the email indicate that it is from a government entity.

In order to minimize the chances of the Malware from being detected, cybercriminals are evolving their infection vector to the next level. They now deploy their Malware in websites and have their victims surf those websites [6], this is known as *drive-by download*.

Malware is not only specifically targeting those in it intends to infect, it is also avoiding those it does not intend to. The early variant of Conficker (Conficker A) will abstain from attacking any computer who had an Ukrainian Keyboard [22]. Also it would prevent itself from attacking any hosts with an Ukraine's IP addresses based on GeoIP database [23].

### D. *Customized Attack Approach*

The types of attacks used by Boutique Malware are customized to suit the environment that it needs to operate to achieve its objectives. Here the intent is to have the attack adapted to suit the operating environment of the targeted to avoid detection while maximizing effectiveness. One such example is the Trojan Horse software, named Trojan.SilentBanker, that specifically targets banking systems with two factor authentication. The Trojan's attack intent is to capture specific sensitive data like names, passwords and account information [17]. Over 400 banks are at risks due to this Trojan [24].

The technique of attack that is commonly used by Boutique Malware is known as Man-In-The-Endpoint (MitE) where the malicious control occurs at the client or local system of the victim. This is different from the notorious Man-In-The-Middle (MitM) attack technique where the interception occurs within the connectivity path between two endpoints. The focus of this MitE is to perform the malicious act prior to entering into the secure HTTPS tunnel[6]. One example is the banking Malware that will modify the transactions made online and send the redirected transfer of funds to an account that attacker has control over. The funds are subsequently retrieved by cybercriminal through the use of money mules. Another is to secretly insert an extra transaction when the victims' transacts online and change the order of the transactions in order not to arouse suspicion [6].

## III. COUNTERMEASURES

Security professionals and researchers have developed many solutions and processes to fend off Malware attacks. There are the Anti-Virus solutions, the layered defence strategy and malware analysis that aids in the development of such defensive solutions. However more work are needed to deal with Boutique Malware.

### *A. Anti-Virus Solutions*

One of the most popular ways to eradicate malicious software is the use of Anti-Virus products. Such products are developed from information or data gathered from past Malware attacks and analyses. Signatures are developed and updated into their products through signature updates. However AUSCERT reckons that 80% of the Anti-Virus solutions are ineffective in detecting and removing Malware [12]. In a report by MessageLab, it noted that out of 31 Anti-Virus companies, only 6 recognized the malicious file to contain a Malware [18]. According another report by Cyveillance [11] a company that does cyber intelligence, they reported that a test conducted on thirteen popular Anti-Virus solutions found that such solutions could detect less than half of the latest Malware threats identified by the company. The report further commented that these anti-malware solutions were dependent on their knowledge of the existence of the Malware. Boutique Malware are not being caught effectively by trips laid out by Anti-Virus companies. An example is the Trojan.Clampi [9] Malware which first existed in 2007 but was only in 2009 that the Malware was detected and acted upon by Anti-Virus solutions [26]. Kotadia [25] commented that if the Malware is targeting only specific individuals or organizations and it is not wide spread, some Anti-Virus companies are less inclined to produce signature updates for them. Boutique Malware could qualify itself to be a zero-day Malware for a prolonged period if the Malware is able to stay away from the radars from Anti-Virus companies. Another challenge posed to Anti-Virus solutions is the pace in which Malware developers change or upgrade their software to evade detection. An example of one such Malware is the Trojan.SilentBanker [8], the percentage of this financial Malware being detected was dropping month by month and this fall could be caused by undetectable variants.

Germain [17] advocates that behaviour based or intelligent forms Anti-Virus technologies are needed to combat such targeted Malware instead of the signature based ones which are dependent on the signature database being adequately updated. Intelligent intrusion detection and prevention systems are commercially available to sift out undesired behaviours rather beyond known threats.

### *B. Layered Security Defence*

The most popular form of security defences against Malware and hackers is to use layered defences or defence in depth strategy. However given the unique characteristics of such Malware with its customized attempts to circumvent security defences, Protas [5] advocates constant evaluation of the security posture. Layered defences should be viewed as an integrated defence structure rather than being viewed individually. Protas further advocates having the ability to correlate security events from the various layers of security defences to detect such Boutique Malware that may have slip through the layers. Security Information Management tools could be used for such intent.

Many organizations conduct vulnerability and penetration assessments on their ICT infrastructure and applications to ensure robustness against possible attacks. Such security assessments are effective in tightening the security layers against possible attacks by Boutique Malware. Another assessment approach can further evaluate the security posture and to identify possible gaps is to use a Malware simulator. An example of such simulator is MalSim [29].

The best way to combat Boutique Malware is to educate the potential targets, that is, the end user [27]. Also, users can be constrained from overriding security rules like installing of software to minimize infection risks [20].

### *C. Malware Analysis*

The effectiveness of any Anti-Virus and layered defence solutions requires having good knowledge of such form of Malware. This comes in the form of Malware Analysis or Malware Analysis reports.

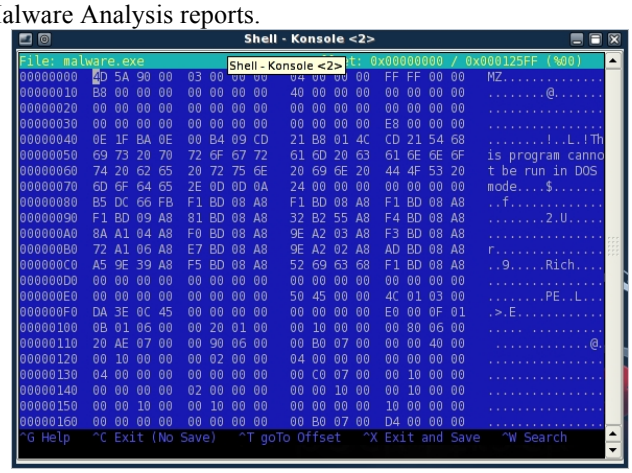


Figure 1 – Malware Analysis

However the analysis of such novel Malware is a major challenge [3] for investigators, anti-Malware developers and researchers. Firstly they are constantly changing or upgrading their software. Secondly, Boutique Malware, like others advanced Malware, are continually adapting their implementation approaches to prevent detection and analysts. Finally, the greatest challenge posed to Malware Analysts is the lack of Boutique Malware samples available for analysis to be done.

## IV. FUTURE RESEARCH

The key area for future research against Boutique Malware is to develop an effective mechanism to detect the infection of such unique malicious software. If these Malware can be detected and its behavior analyzed subsequently, then mitigation plans can be developed to contain the Malware and minimize its risk impacts. Another area to develop is to have a

highly adaptive and flexible defense structure that will include containment measures to counter the Boutique Malware. Such structure will need to be automated in order to adapt quickly to close the gaps exploited and to intelligently sift out anomalies from the seeming regularities while keeping the number of false positives or negatives low.

Our research project focuses on the containment of potential Malware attacks. According to Verizon's 2010 Data Investigation Breach Report [34], it is noted that typically it takes minutes for infection but a significantly longer time in terms of days to months to contain a Malware infection. This poses more risks to the victim in terms of data loss, and loss or limited control over the infected computers. The project intent is to identify the key attributes of notoriously successful Malwares that have affected the community. They are then used to develop a solution that uses similar approaches to counteract and to contain this malice. The project will propose and develop plans and strategies against the identified attributes of the Malwares.

## V. Conclusion

From the earlier years to the most recently, widely publicized Malware like Conficker and Storm were the focused threats that the community needs to deal with. Now a new form of Malware is surfacing and is being used increasingly. Like weapons used in modern warfare, such Malware is evolving from weapons of mass destruction to smart bombs that hits specific targets. According to a report by Security Park [28], the volume of such Boutique Malware will continue to grow yearly. One report advocates a threefold increase of such Malware within a year [30]. Two questions to consider – could the earlier forms of Malware be a test bed for this new form of Malware? Are the cybercriminals quietly developing arsenals that the community is not ready to defend itself against?

With the Boutique Malware, the Internet connected world is dealing with a threat that may originate from anywhere and that may exploit yet to be known vulnerabilities. This may be the unknown risks that would qualify Donald Rumsfield's well known phrase. The IT community urgently needs to develop measures to deal with this risk before it takes full control and users are not able to detect or prevent it from doing so.

## References


[1] N. Gilman, "Hacking goes pro", Feb. 16, 2009. [Online]. Available: http://kn.theiet.org/magazine/issues/0903/hacking-goes-pro-0903.cfm. [Accessed Sep. 3, 2009].

[2] E. Kaspersky, "The Cybercrime Ecosystem", Kaspersky Lab, 2008.

[3] N. Lanelli and R. Kinder, "The Use of Malware Analysis in Support of Law Enforcement", CERT Coordination Center, Carnegie Mellon University, Jul. 11, 2007.

[4] M. V. Horenbeeck, "Targeted Attacks", Sept. 2007. [Online]. Available: http://www.daemon.be/maarten/targetedattacks.html. [Accessed Sep. 4, 2009].

[5] A. Protas, "The rise of targeted malware", SC Magazine, Jun. 26, 2008. [Online]. Available: http://www.scmagazineus.com/the-rise-of-targeted-malware/article/111769/. [Accessed Sep. 4, 2009].

[6] R. Schouwenberg, "Attacks on Banks", Viruslist.com, Oct. 23, 2008. [Online]. Available: http://www.viruslist.com/en/analysis?pubid=204792037. [Accessed Sep. 4, 2009].

[7] Creative Commons Attribution, "Targeted Bank Malware", Securology, Creative Commons Attribution, Jan. 15, 2008. [Online]. Available: http://securology.blogspot.com/2008/01/targeted-bank-malware.html. [Accessed Sep. 4, 2009].

[8] Symantec, "Trojan.SilentBanker", Symantec Security Response, Symantec, Dec. 17, 2007. [Online]. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2007-121718-1009-99. [Accessed Sep. 4, 2009].

[9] Symantec, "Trojan.Clampi", Symantec Security Response, Symantec, Jan. 16, 2008. [Online]. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2008-011616-5036-99. [Accessed Sep. 4, 2009].

[10] G. Masters, "Bank on it: An end to anti-virus", SC Magazine, Nov. 17, 2008. [Online]. Available: http://www.scmagazineus.com/bank-on-it-an-end-to-anti-virus/article/121078/. [Accessed Sep. 4, 2009].

[11] Cyveillance, "Cyveillance Testing Finds Leading AV Vendors Not Keeping Pace with Influx of Malware and Phishing Attacks", Cyveillance, Aug. 17, 2009. [Online]. Available: http://www.cyveillance.com/web/news/press_rel/2009/2009-08-18.asp. [Accessed Sep. 7, 2009].

[12] M. Kotadia, "Eighty percent of new malware defeats antivirus", ZDNet Australia, Jul. 19, 2006. [Online]. Available: http://www.zdnet.com.au/news/security/soa/Eighty-percent-of-new-malware-defeats-antivirus/0,130061744,139263949,00.htm. [Accessed Sep. 7, 2009].

[13] R. Naraine and D. Danchev, "Targeted malware attack against U.S. schools intercepted", ZDNet, Sep. 17, 2008. [Online]. Available: http://blogs.zdnet.com/security/?p=1922. [Accessed Sep. 7, 2009].

[14] The Chosun Ilbo, "S.Korean Army Officers Hit by N.Korean Spyware", Digital Chosunilbo (English Edition), Sep. 2, 2008. [Online]. Available: http://english.chosun.com/w21data/html/news/200809/200809020027.html. [Accessed Sep. 7, 2009].

[15] F-Secure, "Targeted Malware Attacks Against Pro-Tibet Groups", F-Secure, Mar. 21, 2008. [Online]. Available: http://www.f-secure.com/weblog/archives/00001406.html. [Accessed Sep. 7, 2009].

[16] J. Hruska, "CEO perks: stock options?and specially targeted malware", arstechnica.com, Apr. 16, 2008. [Online]. Available: http://arstechnica.com/security/news/2008/04/ceo-perks-stock-optionsand-specially-targeted-malware.ars. [Accessed Sep. 7, 2009].

[17] J. M. Germain, "Boutique Malware: Custom-Made for the Executive Suite", Mac News World, Jun. 23, 2007. [Online]. Available: http://www.macnewsworld.com/story/must-read/57987.html. [Accessed Sep. 7, 2009].

[18] A. Shipp, "MessageLabs Intelligence Special Report:Targeted Attacks April 2007", MessageLabs, Apr. 2007.

[19] B. Acohido, "Clampi virus targets companies' financial accounts", USA Today, Jul. 30, 2009.

[20] A. Greenberg, "Cybercrime's Executive Focus", Forbes, Jun. 11, 2009. [Online]. Available: http://www.forbes.com/2009/06/11/security-cybercrime-executives-intelligent-technology-security.html. [Accessed Sep. 8, 2009].

[21] iDefense Labs, "Spear Phishing and Whaling Attacks Reach Record Levels", iDefense Labs, Jun. 7, 2008. [Online]. Available: http://labs.idefense.com/news/press/bbb/. [Accessed Sep. 8, 2009].

[22] F. Manjoo, "The Worm That Ate the Web", Slate, Mar. 30, 2009. [Online]. Available: http://www.slate.com/id/2214970/. [Accessed Sep. 8, 2009].

[23] P. Porras, H. Saidi and V. Yegneswaran, "An Analysis of Conficker's Logic and Rendezvous Points", SRI Internetional, Mar. 19, 2009. [Online]. Available: http://mtc.sri.com/Conficker/. [Accessed Sep. 8, 2009].

[24] L. O. Murchu, "Banking in Silence", Symantec, Jan. 14, 2008. [Online]. Available: http://www.symantec.com/connect/blogs/banking-silence. [Accessed Sep. 8, 2009].

[25] M. Kotadia, "Antivirus firms battle 'unique malware'", ZDNet Australia, Nov. 26, 2006. [Online]. Available: http://news.zdnet.co.uk/security/0,1000000189,39284845,00.htm. [Accessed Sep. 8, 2009].

[26] E. Millis, "Clampi Trojan stealing online bank data from consumers and businesses", CNet News, Jun. 29, 2009. [Online]. Available:

http://news.cnet.com/8301-27080_3-10298233-245.html. [Accessed Sep. 8, 2009].
[27] Avira, “Avira warns: targeted malware attacks increasingly also threatening German companies”, Avira, Jul. 25, 2007. [Online]. Available: http://www.avira.com/en/security_news/targeted_attacks_threatening_companies.html. [Accessed Sep 8. 2009].
[28] Security Park, “Increase in malware volume and sophistication’, Security Park, Sep. 18, 2007. [Online]. Available: http://www.securitypark.co.uk/security_article259909.html. [Accessed Sep 16. 2009].
[29] R. Leszczyna, I. N. Fovino and M. Masera, “Simulating malware with MAlSim”, Journal in Computer Virology, Springer Paris, Jul. 1, 2008.
[30] C. Everett, “Malware variant trend reflects police action”, ZDNet, Jun. 1, 2005. [Online]. Available: http://news.zdnet.co.uk/security/0,1000000189,39201363,00.htm. [Accessed Jan 2, 2010].
[31] R. Westervelt, “Enterprise botnets contain thousands of malware variants”, SearchSecurity.com, Oct 15, 2009. [Online]. Available: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1371414,00.html. [Accessed Jan. 2, 2010].
[32] P. Roberts, “Targeted malware attacks: The new normal”, InfoWorld, Jul. 29, 2010. [Online]. Available: http://www.infoworld.com/t/hacking/targeted-malware-attacks-the-new-normal-159. [Accessed Sep. 24, 2010].
[33] D. Geer, “Advanced persistent threat”, NetworkWorld, Apr. 12, 2010. [Online]. Available: http://www.networkworld.com/news/tech/2010/041210-tech-update.html. [Accessed Sep. 24, 2010].
[34] Verizon, “2010 Data Breach Investigations Report”, Verizon Business, Jul. 28, 2010. [Online]. Available: http://newscenter.verizon.com/press-releases/verizon/2010/2010-data-breach-report-from.html. [Accessed Sep. 23, 2010].