Institution: University of Birmingham

Unit of Assessment: UoA 11, Computer Science and Informatics

Title of case study: Fighting the Malicious Web

Period when the underpinning research was undertaken: 2010–2014

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	Role(s) (e.g. job title):	Period(s) employed by submitting HEI:
Dr Marco Cova	Lecturer in Computer Science	2010–2014

Period when the claimed impact occurred: 2014–present

Is this case study continued from a case study submitted in 2014? No

1. Summary of the impact

Malware (malicious software) is one of the top security issues with today's internet, and there is a growing trend of advanced malware that camouflages itself in order to evade standard detection tools. Dr Marco Cova developed novel methods of detecting advanced, evasive malware at scale. As a result of this work, Cova became a founder member of the company Lastline, where his research has **contributed to innovation and entrepreneurial activity through the design and delivery of new products**, specifically the development of sophisticated anti-malware products that have won dozens of industry awards. Cova's work has significantly **improved the performance** of Lastline's anti-malware products, establishing Lastline as one of the fastest growing cyber-security companies in the world, **stimulating direct investment** of over US$52 million. Products using Cova's technology now protect more than 20 million individual users, including schoolchildren and callers to emergency services, as well as international banks and Fortune 500 companies.

2. Underpinning research

Cybercrime has become a major threat to businesses and organisations. Accenture, in their 2019 "Ninth Annual Cost of Cybercrime Study", estimate the total value at risk from cybercrime over the next five years to be US$5.2 trillion, with a quarter of this threat coming from malware [S1], much of which is delivered via webpages. In recent years, there have been numerous high-profile attacks on UK businesses, universities and the NHS. Basic malware can be easily detected and stopped by anti-virus systems that scan files for patterns of bytes that act as a fingerprint for known malware. In response, malware authors have developed malware that can encrypt and camouflage itself, completely evading basic scans. Additionally, the most dangerous malware will use attacks that have never been seen before and so have not been fingerprinted by anti-virus companies. Such advanced evasive malware represents a major threat to businesses and organisations. Cova's research has led to **improved performance** and **new products** for stopping such malware, which are actively used by a wide range of organisations.

The research conducted at the University of Birmingham (UoB) since 2010 has focused on pioneering systems for efficiently detecting and analysing advanced, evasive malware on a large scale. Cova was the key researcher at UoB on two projects (2010–2014) that developed anti-malware systems that are now widely used: PROPHILER [R1] and REVOLVER [R2]. The PROPHILER system enables the analysis of malicious web content at a scale that was previously impossible, whilst REVOLVER provides techniques for the automated detection of malware that will evade other scans.

Individual webpages can be scanned to detect malware in tens of seconds. However, modern websites may contain hundreds of pages, and to proactively find malware on the internet requires hundreds of millions of pages to be scanned. Before PROPHILER, such scanning was impossible; PROPHILER reduces the resources required for performing large-scale analysis of malicious web pages by developing a fast and reliable filter that can quickly discard pages that are benign, forwarding to the costly analysis tools only the pages that are likely to contain malicious code. **Key research findings** made by Cova as part of the PROPHILER project were:

1. Identifying key features of a webpage that characterise what the website does;
2. Developing a method of statically analysing complex webpages to automatically detect these features at very large scale;
3. Applying machine learning techniques to these features to determine if a web page is likely malicious or benign.

Putting these three steps together: PROPHILER [R1] statically models a web page using a set of features designed to characterise the page's security aspects. It then compares these features against profiles established on datasets of benign web pages; if the analysed page deviates significantly from the established profiles, it is deemed potentially malicious. Cova's research showed that this fast filter method was effective at scanning millions of webpages and so finding malware on a scale that was previously impossible. This **improved performance** has led directly to **new products** for Lastline; the method is used by Lastline's main product Lastline Defender [S2] as part of a fully automated system to find and stop new sources of malware.

The creators of malware have responded to such malware detection systems by making their malware deliberately hide from scanners, adding methods to the malware that try to detect if the scanner is being executed by a human on a normal computer or by a scanning program. REVOLVER developed a technique to automatically identify evasions in web pages. Cova's key new research idea was that evasive malware will contain snippets of code similar to other non-evasive malware, whereas benign webpages will not. REVOLVER [R2] finds pairs of pages that are similar and that have been classified differently (one malicious and the other benign). This different classification outcome is often attributable to the use of an evasion technique by the malware that, once identified, can be analysed, and scanning methods developed to defeat it. This **further key finding** is the **contribution to innovation** which made it possible to detect advanced malware that would evade other scans.

Performing this work required a deep understanding of website malware, large-scale static analysis and machine learning; a combination that Cova pioneered. The results of this combination were the first effective methods of detecting malware that could be used on the scale of the internet and a technology that has given Lastline a key competitive edge as an anti-malware company.

3. References to the research

R1. Davide Canali, Marco Cova, Christopher Kruegel, and Giovanni Vigna (2011). "Prophiler: A Fast Filter for the Large-Scale Detection of Malicious Web Pages", International World Wide Web Conference (WWW), 2011. DOI: 10.1145/1963405.1963436.

Microsoft Academic Search ranks WWW as a top conference in World Wide Web research; the Australian CORE association ranks WWW as an A* conference.

R2. Kapravelos, A., Shoshitaishvili, Y., Cova, M., Krügel, C., and Vigna, G. (2013). "Revolver: An Automated Approach to the Detection of Evasive Web-based Malware". Proceedings of the USENIX Security Symposium, 2013. ISBN 978-1-931971-03-4.

The Australian CORE association ranks this conference as an A* conference, and it is one of the leading venues for cyber security research.

4. Details of the impact

Malware (malicious computer code) is one of the biggest threats to the internet; for instance, the Zeus malware steals hundreds of thousands of credit card numbers every year, and, in 2017, the

WannaCry ransomware malware crippled organisations across the world, including the NHS. Anti-virus companies have developed effective ways to detect and stop single infections by well-known malware on a single computer, however, to proactively find and defend against new, advanced malware infections from websites, new unknown malware must be detected and millions of websites must be scanned.

Developing a new product that improves online security

Cova's research made fundamental steps in solving these challenges, **contributing to innovation and entrepreneurial activity through the design and delivery of new products**. In 2014, Cova moved full-time to the company Lastline in order to commercialise his research, which resulted in Lastline's flagship Lastline Defender product [S3] that proactively defends organisations from malware, including new and evasive malware.

Lastline Defender is a practical tool that can proactively detect and stop highly advanced, evasive malware. This new product has stopped very damaging attacks against a wide range of large companies, including potentially devastating ransomware attacks [S4]. Lastline's product is often ranked as the best by independent testers [S5]. Cova's research was key to making this product viable, as the Chief Technological Officer and co-founder of Lastline writes:

> Dr Cova's technologies allow us to process possible malware several orders of magnitude faster than would otherwise be possible. His research has been the cornerstone of our efforts to detect evasive malware that is becoming increasingly common and cannot be detected by normal scanning methods. Dr Cova's research has made a fundamental contribution to our current product line. [S6]

In another testimonial, the Chief Product Officer and co-founder of Lastline writes:

> A key insight provided by Dr Cova's Revolver work was that evasive malware could be detected by looking for code that is shared, or similar to, other known malware. The contribution of the Revolver work was to show that this works in practice, and it is now a technique we use to scan millions of documents every year […] We considered this research so important to the success of our company that we took every effort to ensure that Dr Cova joined Lastline as part of the founding team. [S7]

Products that use Cova's technology are used by 1,000s of customers across the world including telecoms providers, payment card processors, shipping companies and global banks, to protect more than 20 million individual users [S4, S5]. Lastline has worked with more than 20 leading security product providers, including some of the biggest anti-virus companies such as Sophos and Symantec [S8] to ensure that products that use Cova's technology can be integrated with their offerings. The consulting companies KPMG, PWC and Dell Secureworks have all recommended Lastline products to their customers and seven leading managed security service providers use Lastline's product [S8].

Improving security performance to enable global product adoption

In a leading 2018 study, **Lastline's product detected 100% of the evasive malware tested**, unlike products from some of the largest advanced malware detection companies, such as FireEye, whose product detection rate was only 80%. A key reason for Lastline's excellent performance was the technique for identifying evasive malware presented in Cova's REVOLVER research [R2]. Lastline's product also proved to be one of the most cost-effective advanced malware detection solutions. A key reason for this is the fast filtering techniques developed by Cova in his PROPHILER research [R1].

These extremely strong test results for the implementation of Cova's research are borne out by first-hand accounts from Lastline's customers. The **product has been adopted for use in multiple sectors worldwide**, protecting banking and finance, aerospace, education,

telecommunications, maritime security and the media. For example, the chief security architect at the Gwinnett County school board in the US, who uses Lastline Defender to protect 190,000 students, teachers and administrators, writes:

> Lastline provides us with deeper visibility and insight into web downloads and malicious attachments embedded within 'accepted' business applications and protocols, and 'passed-through' by traditional perimeter security solutions. Lastline also provides us with 'post-infection' awareness to quickly detect and remediate compromised endpoint systems that are 'calling home' to criminal networks. [S9]

One of the largest wireless telecommunications networks in the United States who uses Lastline to protect services to millions of customers and 911 emergency service calls writes:

> The corporate email security team loves Lastline because it catches stuff that two of our other security solutions miss. When I was looking for a sandbox utility for email, I performed a side-by-side comparison between Lastline and those other tools. Lastline outperformed both of them by a large margin. [S10]

The Head of Service at GTMaritime (a maritime communication company) writes:

> Within days of the launching GTMailPlus, we felt the service from Lastline was so security critical, we now integrate the Lastline solution as a compulsory element of our service. We are in the process of rolling this out to our entire customer base, so we are assured our end-users and systems are protected. It's 'win-win' all around. [S10]

Other customer case studies and quotes can be found on our supporting website [S10].

The take up of Lastline is further evidenced by its success as a company. Since Cova joined Lastline in 2014, it has grown to over 100 employees and received direct investment of US$52.5 million, including funding from Dell and the venture capital firms e.ventures and Redpoint Ventures [S11]. Lastline has won dozens of industry awards for the performance of its product, these include, in 2018 alone, awards for "Most Promising Cybersecurity Provider", "Game Changer of the Year" and "Best Network Protection" [S12]. Inc. magazine named Lastline, "the leader in advanced threat protection", eighth among security companies on its 37th annual Inc. 5000, "the most prestigious ranking of the nation's fastest-growing private companies" [S13].

5. Sources to corroborate the impact

S1. Accenture Security, The Cost of Cybercrime, 2019 [accessed 25.02.2021]

S2. Lastline, Network Detection and Response Platform [accessed 25.02.2021]

S3. Lastline, Lastline Defender: AI-Powered Network Security, 2019 [accessed 13.11.2020]

S4. Lastline, Detecting Ransomware Using Behavioral Analysis [accessed 13.11.2020]

S5. Lastline Blog, Lastline Ranks Highest in Security Effectiveness in NSS Labs Breach Detection Systems Group Test – Again, 2017 [accessed 13.11.2020]

S6. Testimonial from Lastline, Chief Technological Officer

S7. Testimonial from Lastline, Chief Product Officer

S8. Lastline, Industry Partners [accessed 13.11.2020]

S9. Gwinnett County Public Schools Defends Against Advanced Malware with Lastline Enterprise – Case Study [accessed 7.12.2020]

S10. Lastline Supporting Evidence Website (case studies and quotes from the following: A Global Bank, A Technology Company, Fin Tech Services, GTMaritime, Lastline Detonator, Aerospace, Education, CorporateFactSheet, TeleComms Company, A Managed Security Service Provider, Major Card Processor, Media Conglomerate)

S11. Crunchbase, Total Funding Overview [accessed 13.11.2020]

S12. Lastline Awards [accessed 13.11.2020]

S13. Inc. 5000 List of America's Fastest-Growing Private Companies, Lastline Ranks Among Top 10 Security Companies on the 2018 [accessed 13.11.2020]