



**OXFORD
BIOCHRONOMETRICS**
STOP FRAUD STAY RELEVANT

Oxford BioChronometrics, LLC
www.oxford-biochron.com
29 South Willow Street
Montclair, NJ 07042

February 12, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
Attn: Evelyn L. Remaley
Deputy Associate Administrator

Re: A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats [Docket No. 180103005–8005–01]

Dear Deputy Associate Administrator Remaley,

Thank you for the opportunity to comment on the draft “Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats.” We commend the Departments of Commerce and Homeland Security (Departments) for their excellent work in drafting a comprehensive view of the problems posed by botnets and other automated, distributed threats. We also applaud the open and multi-step process that allowed stakeholders and other interested parties to engage and provide input as the agencies crafted their report.

Oxford BioChronometrics agrees with the Departments’ approach in looking holistically at the problems posed by increasing and more effective use of existing and new forms of automated, distributed attacks, including botnets. We further commend the Departments for offering a broad-based menu of options and efforts. However, Oxford BioChronometrics thinks that the Departments should more strongly emphasize the importance of effective, adaptable authentication, which, in our view, is one of the key means of combatting bots. If bots and other forms of attack can be distinguished as non-human or otherwise malicious, then defenders have the opportunity to respond appropriately.

Oxford BioChronometrics believes that greater emphasis on biometrics of the sort that cannot be easily spoofed or faked will help cyber defenses better manage the problems posed by botnets and other distributed forms of attack. However, we do not think authentication more sophisticated than multifactor authentication (MFA) is a silver bullet for these problems. Rather, behavioral biometrics deserve greater emphasis in the menu of solutions the Departments are considering. Consequently, we agree with the Departments that “[n]o single investment or activity can mitigate all harms, but organized discussions and stakeholder feedback will allow us to further evaluate and prioritize these activities based on their expected return on investment and ability to measurably impact ecosystem

resilience.” We believe that a summary of how our technology works may prove useful for the Departments.

Oxford BioChronometrics’ Background

Oxford BioChronometrics is a cybersecurity company that provides a proven new way to protect digital assets – from ads to networks, individuals to communities, in the advertising, finance and health industries. The company emanates from the University of Oxford Software Incubator, and the University still owns a stake in the company. Put simply, our technology measures life signs (behavior) over time, in real time:

Bio=Life

Chrono = Time

Metrics = Measurements

The background of our tech team has been cybercrime and protecting applications such as internet banking from advanced bots. This enabled us to get lots of experience with the most sophisticated bots and botnets around – experience that is kept current by wide use in the field of advertising, which is overrun with bot fraud. Using sophisticated behavioral biometrics, we help companies do the hard work of detecting humans (as opposed to bots), which saves companies billions of dollars in costs associated with fraud.

Technology

Oxford BioChronometrics places our analytics code on the server or site to be protected and can stream behavioral data to the backend. Focusing on behavior, not past performance or identity, over 1000 browser quirks, properties and features are collected, from client specific settings like keyboard layout, time zone, languages, color depth, etc. to movement patterns, to CPU speed and device ID. Analyzing all of these together against a statistical model creates a behavioral profile which can be used as an implicit authentication of the user as a human or non-human, including exactly what type of non-human actor is attempting to access the digital asset (site, page, ad, etc.).

Why Botnet Detection is Difficult

Most solutions rely, in part, on past performance of an Internet Protocol (IP) address. An IP address can represent a single device on the internet, but it can also be a proxy server for a company, or a router's IP address for a family. All devices linked to the internal network using WiFi communicate to the internet through the router and thus are using the IP address of the router. For a family using the same router, and the son or daughter has a mobile phone with some software installed on it, like a free game from the store which runs ads in the background, that device gets infected with adware. This means that the family IP address has both bots (from that compromised device) and humans (from the other devices) viewing ads. This also can be true for 4G networks with lots of devices sharing a (gateway) IP address, Wi-Fi hotspots at restaurants, etc. where a mix of devices connect to the internet. So, using an IP address to identify botnets will likely have mixed results, which means filtering by IP addresses is simply ineffective and will always be so, especially as botnets continue to infect the devices of an uninformed or unaware user.

Strategies for Bot Detection

We start with our collection code – a call to an encrypted JavaScript. The encryption prevents bots from changing the JavaScript code using find & replace before the page is loaded and executed in the browser. The JavaScript code will perform technical tests which validate fundamental characteristics

of the client and browser. A way we like to think about how this works is suppose one is talking about cars, say, a Ferrari. It may look like a Ferrari, and others may tell you it's a Ferrari, but our technology can see if it's actually a Volkswagen. In that vein, our script will not ask what brand and/or type car it is, instead it measures the length, width, weight, number of cylinders and wheelbase, etc. and from these numbers we are able to infer which brand, type, or year it really is.

Our tag enables us to determine whether the page has been viewed by human or bot based on characteristics which bots do have and humans do not have. For example, headless browsers (browsers without a graphical onscreen window) have certain intrinsic characteristics which can be detected, as the rendering of graphical items works differently. Moreover, our tests will work on any type of device or page, static AD, dynamic AD, video, in-app on mobile phones, tablets, (using web view), or in a browser on a desktop, laptop or tablet.

Bot networks tend to target high-volume areas in order to make the most money through fraud with as little effort as possible. Bots that are able to view an ad (impression), click on the ad (click-through) and then fill in a form (conversion) are sophisticated bots which are expensive to develop. They are well-designed for conducting fraud, as their sophistication makes them expensive to detect. Their developers invested a lot of time to try to make the bots behave like humans. Of course, every time a botnet is taken down, or bad traffic is blocked, the same or new bots owners will come back with more sophisticated bots.

In order to address this, an end-to-end continuous study should be conducted. This would allow the measurement of the number of impressions, click-through rate and the moment of conversion at the confirmation page. Such a study will enable Oxford BioChronometrics to see and track bots through the process. It would also enable us to track and detect new advanced bots which are able to fraudulently engage in the entire advertising chain, from impression to conversion.

General Methods of Detecting Bots

Detecting non-human internet traffic requires the simultaneous application of a range of techniques, to ensure that coding, sensor, statistical or extrapolated data are free from module or systemic errors. The premise upon which detection occurs relies on empirical evidence of the behavior (or functional capabilities) of the human or bot device requesting the ad impression, as opposed to any previously compiled device or IP-address black-list or, Bayesian probability model based upon speed, time or geo-location. This detection takes the form of a series of tests that the device will encounter as part of its normal execution path in loading the ad-impression. If any of the tests fail, it becomes an indicator of the limitations of the bot-device.

Through significant prior observation (bot-device traffic in the range 10^9), Oxford BioChronometrics knows that bot-devices employ only the minimum necessary capabilities to register an AD impression, due to the combined economics of ad impression volume pricing, CPU processing power & network traffic costs. Because the volume necessary to create a small economic benefit is extremely large, the bot-device must limit the CPU and network traffic that it generates to a minimum, as otherwise it cannot create a net economic benefit to the operator of the bot-device.

It does this by using Reduced-Function JavaScript engines and significantly older virtualized web browser versions. Sometimes it will skip executing embedded URLs or JavaScript code-blocks altogether during the loading of an ad-impression, if it does not believe these items are relevant to acquiring the ad-impression economic benefit. For this reason, Oxford BioChronometrics introduces specially crafted URLs and JavaScript code-blocks into our SecureAd code (which would always be executed by a human-device), that allow us to test a variety of different bot-device capabilities, from

which we determine if the ad-impression was initiated by a human-device or a bot-device, and if a bot-device, what type.

Other Considerations

Oxford BioChronometrics would offer the following additional observations for the Departments to consider:

- Substantive evidence of the efficacy of our detection algorithms is provided through a series of validation models that ensure the detection is accurate. Unrelated non-human traffic characteristics are chosen that, on their own, are not sufficiently strong enough to enable detection, but can corroborate predetermined detection data sets and provide strong proof-of-correctness models. These might include combinations of the distributions of user agents, ip addresses or CPU performance models, etc.
- When we analyze the occurrence of IP addresses (i.e. the number of times we see a specific IP address), we see that daily single-use IP addresses are more often found in human traffic than in non-human traffic, reflecting that real traffic is naturally more varied than artificial traffic. However, traffic sourced from a botnet, as opposed from a few bots running on a small server farm, would start to display the same (or close to) the natural variance of human traffic, depending on the ratio of the size of the botnet to publisher's web traffic volume.
- What might betray the almost-human like traffic (as being truly non-human), is the distribution of local CPU performance metrics across the traffic. Human traffic distribution should spike at 4-12 milliseconds for a specially crafted block of jCRIPT JavaScript and also again at 325-350 milliseconds, while non-human traffic shows a relatively linear distribution without these outliers.

Third Party Validation

Oxford BioChronometrics' approach to authentication has been validated by a number of third parties, including:

- NATO: Oxford BioChronometrics was singled out in the NATO Defense Innovation Challenge¹ for its technology to detect the “weapon of choice” for state-sponsored cyber-attacks, known as Remote Access Trojans. Such attacks are otherwise undetectable by other technology until after they have happened. The company's unique ability to analyze behavior in real time, which it calls its Human Recognition Technology, can be used to protect digital assets of all types, whether they are complex secure networks or digital advertisements.
- Method Media Intelligence: In a recent independent, blind comparison test by ad fraud researcher Shailin Dhar of Method Media Intelligence², Oxford BioChronometrics was named “the best performing ad fraud detection solution” by detecting 91% of all bots – more than twice as effective as the market leader.

Additionally, an Oxford BioChronometrics' study³ was cited in a letter⁴ sent by Senators Mark Warner (D-VA) and Chuck Schumer (D-NY) to the Federal Trade Commission (FTC) regarding the size and scope of digital ad fraud.

¹ <http://oxford-biochron.com/oxford-biochronometrics-wins-nato-defense-innovation-challenge/>
<https://www.ncia.nato.int/NewsRoom/Pages/170404-NITEC17-Innovation-Challenge.aspx>

² <https://www.slideshare.net/ShailinDhar/mystery-shopping-inside-the-adverification-bubble>

³ https://oxford-biochron.com/downloads/OxfordBioChron_Quantifying-Online-Advertising-Fraud_Report.pdf

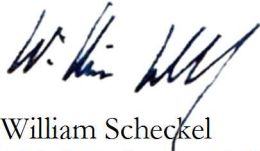
⁴ <https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=2754B7B1-5B12-4CE8-BE26-3BAE7A8B6142>

Conclusion

Oxford BioChronometrics would like to reiterate that combatting botnets and other distributed attacks will require multiple lines of efforts among the public and private sectors. However, we would emphasize the importance of identifying bots and similar attack methods as early as possible. To this end, we suggest greater emphasis on authentication methods more sophisticated than those currently in wide use.

Please do not hesitate to contact us should you require additional information or have any questions.

Regards,

A handwritten signature in black ink, appearing to read 'W. Scheckel', with a stylized flourish extending from the end.

William Scheckel
Chief Marketing Officer
Oxford BioChronometrics, LLC