News, Resources and Useful Information for the Online Investigative and OSINT Professional from Toddington International Inc.

Toddington International Inc.

Online Research and Intelligence Newsletter

JANUARY 2019 EDITION

In This Edition

Welcome to the Newsletter

Welcome to our first newsletter of 2019. We wish all of our clients, colleagues, and friends the very best for the year ahead!

In this edition of the newsletter, **Justin Seitz** provides some important advice on **"How To Blow Your Online Cover with URL Previews"**. In this article, Justin explains how a simple and common mistake could reveal an investigator's network connection, possibly alerting a subject to the fact that they are under investigation.

Also in this newsletter, we are pleased to provide links to some of the many online investigative and security tools we have been exploring and using lately, and just a few of the OSINT-related articles we have found of particular interest.

With a busy year ahead, we are pleased to welcome the newest member of the TII team, **Sabreen Dhaliwal**. Sabreen comes to us as a graduate of the University of Fraser Valley's Criminology program and will serve as Office Manager at our Vancouver Headquarters. Sabreen will be providing daily support for our domestic and international operations, including the ongoing development of our growing

E-Learning Graduates

Congratulations to the following students who are among the latest to have successfully completed the 40-hour Using the Internet as an Investigative Research Tool™ e-learning program with TII:

- Stephen Weiss
- Jori-Matti Kock
- Jim Randall
- Grant Cherry
- Liza Zhao
- Lucas Falkiner
- Luís Alves
- Peter Karlsen
- Karen Pitman
- Sara Huntington
- Ricardo Areco
- Melony Rocco
- Carly McMahon
- Janet Cartwright
- Mathew Conner
- Aaron Locke
- Theresa Anderson
- Peter McKinney
- Lilla Trentini
- Dyon Verburgh
- Annot Coulombe
- Holly Bennett
- Saare Yemane

Congratulations to the following students who are among the latest to have successfully completed the 40-hour Open Source Intelligence for Financial Investigators e-learning program with TII:

- Rita Plantera

- Paulo Alves

As we respect the privacy of our students, we only publish the names of students who have provided express permission to do so.

How To Blow Your Online Cover With URL Previews

Photo Credit: wolfgangfoto via Flickr

By Justin Seitz, Hunchly

URL previews are a nice feature found in most messaging applications. They allow you to paste a URL to a friend or colleague, and have a handy miniature view of the website you are about to view.

The downside is that a lot of applications generate these previews without you knowing what is happening behind the scenes. In some cases, this can equate to you disclosing your public IP address in a manner that you likely wouldn't want.

The difference with URL previews in messaging applications is that you are broadcasting to the website owner that you are ***discussing*** the website, as opposed to just browsing to it.

This small and subtle change in context is actually quite an important distinction. You'll see why very shortly…

A Little History

A few years ago, I was on a penetration test where I was attempting to spearphish executives at a well-known corporation in Europe. They had one of the most brilliant CISOs I had ever met and an absolutely amazing incident response team on staff.

After I sent the initial round of phishing emails, I was monitoring my command and control server to look for connections from users, anti-virus, or anything else that might indicate that I was either having some success or was about to be caught.

After a few hours, there was not a lot of activity until my web server received a connection from an IP address that resolved back to Skype. This was a WTF moment for me since my phishing server was brand new and there didn't seem to be a good reason why a Skype server would be touching it.

A few minutes later, another hit from a different Skype server. Now I was really wondering what was going on.

Then it dawned on me. Someone was discussing my command and control system during a Skype chat, and Skype was generating previews of the phishing site I had setup.

I performed a couple of quick tests using my own Skype account, and sure enough, I could reproduce the issue easily. I now knew that the incident response team was on to me, and that it was time to switch tactics.

But this also raised a much larger issue in my mind when it came to online investigations, incident response, and running covert online operations.

How Does This Apply to Online Investigations?

There are two viewpoints here: one is from an investigative standpoint and the second is from the standpoint of you running a covert operation through a website.

fellow investigator, you may end up notifying your target that you are talking about them. This is exactly how I figured out that the incident response team was on to me during my penetration test. You likely don't want this to happen.

The second standpoint is where you are running a website for a covert online operation. You can monitor for these URL previews and determine that someone is discussing your site, potentially letting you know that your ruse is working or that you might be caught out (again, context is important and mission-dependent here).

Either way, it is a unique set of behaviours that can be observed that is not general browsing activity.

Test Results From Various Platforms

I did some quick testing of various messaging clients and services. The test was to simply setup a Python web server on a Digital Ocean droplet ($5/month plan is sufficient). The Python web server just printed out the IP address and headers of the connecting client.

I also setup a DNS record specific for this testing so that I could try using IP addresses vs. domain names. WhatsApp was the only service tested that responded differently for IP addresses vs. domain names. Every other service was happy to generate previews for an IP address. There was also no difference between using an HTTP vs. HTTPS URL.

Here is a summary of findings:

Slack

We, like many other companies, live on Slack so this was the first test I performed. Slack was happy to generate URL previews and identified itself with the following User-Agent:

User-Agent: Slackbot-LinkExpanding 1.0 (+https://api.slack.com/robots)

The IP address of the request was from my publicly facing IP address through my office connection in both mobile and desktop versions of Slack.

Note that you can disable previews in Slack by going to Preferences -> Messages & Media -> Inline Media and Links. Uncheck the "Show text previews of linked websites."

Apple Messages

preview directly from your public IP address as can be expected.

The user agent shows:

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1 Safari/601.2.4 facebookexternalhit/1.1 Facebot Twitterbot/1.0

Pretty interesting that you see the Facebot and Twitterbot pieces in there! This was actually picked up by a Reddit user as well.

Here is where things can get more interesting: if you are sending an SMS phish to a target, you can enhance the URL preview experience a little by ensuring you have a file named:

apple-touch-icon-precomposed.png

The Messages app will attempt to retrieve this file once it determines that it can successfully reach the target web page. This file will be used in the preview that is generated and could help to entice your target to click the link. It can also be a way of acknowledging the fact that Messages was the application doing the URL preview in the first place.

Wire

Wire is pretty interesting. When you post a URL from the app both on desktop and on your mobile phone, your public IP address will show up in the logs. However, there are no User-Agent headers that show up. In fact, the only header that Wire sends is:

Connection: close

So this in itself is interesting because many of your HTTP clients (browsers, crawlers, bots, etc.) will send additional headers. By Wire stomping out all information this does become a "tell" that perhaps someone is discussing a target site in the Wire application. Further tracking of how often you see this limited set of client headers would have to be done in order to come up with something more statistically relevant than my single observation.

Note that in Wire there is a setting in Preferences -> Options called "Create previews for links you send." If you disable this, it will prevent Wire from doing these URL previews. It is recommended you do this.

Facebook

User-Agent: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)

It doesn't use your public IP address but does indicate that someone has posted a link to the target site on their Facebook profile or have sent it via Facebook Messenger. The IP address you see show up will be registered to Facebook so you can use a site like ipintel.io to look it up.

WhatsApp

WhatsApp behaves somewhat differently than the other services. It will not honor IP addresses directly, but if you type in a domain (and any port), it will attempt to do URL previews. Additionally, it will do continuous requests as you type the URL of the target page as well which generates a lot of traffic.

The User-Agent looks like this:

User-Agent: WhatsApp/0.3.1649 N

The request comes from your public IP address.

Skype

During original testing, Skype was not producing URL previews. Subsequent testing revealed this was due to a non-standard web server port being used in the testing. Further testing of Skype revealed that be default, it still does produce URL previews, providing the website has a proper domain name and is listening on the standard ports of 80/443.

The User-Agent looks like this:

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) SkypeUrlPreview Preview/0.5

The request comes from an IP address owned by Microsoft.

Note that you can disable this by going into Preferences -> Messages and disabling the "Web link previews" option.

Services That Didn't Generate Previews

There were some services that didn't generate any previews or traffic when pasting links, or typing URLs. Of course you should test this yourself to verify.

Sudo (Mobile)
Threema (Mobile)
Twitter DM (Mobile/Web)
Wickr (Desktop)

All of the mobile testing was done on an iPhone X so there may be differences with Android that aren't covered here.

There are probably a ton of other messaging apps out there that you could test, and you absolutely should. Feel free to let me know and I can update this post with your results.

Mitigations

There are a few things you can do to help mitigate the risk:

Defang your URLs: This is simply the method where you replace the dots and colons with other characters, or use brackets. An example could be:

Regular: https://www.hunch.ly

Defanged: hxxps://www[.]hunch[.]ly

Use a VPN: This is a secondary suggestion really as it is isn't mitigating the original problem, but for the services that are spitting out your public IP address, this will at least obscure it.

About the Author: Justin Seitz is the creator of Hunchly, a web capture tool designed for online investigations. Hunchly automatically collects, documents, and annotates every web page visited, creating a transparent audit trail for online investigations. To learn more, visit www.hunch.ly. To view the original article posted on the Hunchly blog, please visit https://hunch.ly/osint-articles/osint-article-how-to-blow-your-online-cover.

Investigating Insurance Fraud Online

This specialized course will enable investigators, case managers, and other fraud-prevention and insurance professionals to effectively use the internet as an investigative tool in order to locate case-specific information, both quickly and efficiently, reducing the time and resources expended on everyday investigations.

February 25-26, 2019, Vancouver, BC

Advanced Internet Intelligence & Online Investigations

Aimed at managers, frontline investigators, researchers, and analysts alike, this advanced training program will provide detailed instruction on effectively using the Internet as an Open Source Intelligence, research, and investigation tool. Demonstrating advanced search and analysis techniques for mining Web-based and social media information, this comprehensive training program will also examine a number of essential privacy tools for ensuring data, communication, and online security. Techniques being used by the criminal element to conceal their identity, location, and illegal behaviour will also be introduced.

March 18-19, 2019, Toronto, ON

March 25-26, 2019, Vancouver, BC

Social Media Intelligence & Investigation

To recognize, collect, and leverage the value of social platform-sourced information, research and investigative professionals must fully understand the restrictions and implications of obtaining and utilizing such information in a manner that does not violate user privacy expectations, license agreements, and other legal limitations. This course will introduce research and investigative professionals to a variety of innovative tools and techniques that will enable you

and appropriately.

May 16-17, 2019, Vancouver, BC*

June 6-7, 2019, Toronto, ON*

**Only a limited number of seats are available at the early-bird rate, based on a first come, first served basis. Sign up early to receive the discounted pricing.*

Australia-Based Training

We will also be in Australia for training in the upcoming months. For dates, locations, and pricing information, please contact us.

TII is pleased to offer a number of specialized and customizable in-house training programs for both the public and private sector in a variety of formats. We also have available a number of expert speakers available. To learn more about what we can do to empower your workforce, contact us.

Resources for the OSINT Professional

https://www.insecam.org - Directory of unsecured online surveillance security cameras

https://chrome.google.com/webstore/detail/un-delete-reddit-comments - Chrome extension that allows users to save a cached copy of Reddit pages

https://pitoolbox.com.au/new-facebook-tool - Interesting tool that compares two Facebook profiles to determine similarities or connections

http://pitoolbox.com.au/facebook-tool - Uncover as much information about a Facebook profile, including open source information usually hidden by Facebook

https://online.maryville.edu/blog/the-online-students-research-toolkit - The Online Students' Research Toolkit (from Maryville University)

and traceroutes, among other DNS searches

Web proxies useful for accessing blocked websites and anonymous/private browsing:

https://hide.me

https://www.hidemyass.com/proxy

https://www.privoxy.org

https://www.filterbypass.me

https://www.proxysite.com

https://29a.ch/photo-forensics – Digital image forensics tool that provides comprehensive meta data and offers various image analysis tools

https://www.shodan.io – Search engine for internet-connected devices

https://1.1.1.1 – Protect your privacy by using this fast and anonymous DNS server

http://onion.link – Search engine that enables access to Tor's onion sites

https://livingatlas.arcgis.com/wayback – A digital archive of the World Imagery basemap powered by ESRI that enables users to access satellite views of nearly any location on the planet over multiple years

https://www.earthcam.com – Live webcams from around the world, searchable by location

https://www.makeuseof.com/tag/best-google-search-tips-pdf – Google cheat sheet of search operators and commands

https://www.zotero.org – Tool for collecting and organizing webpages for later sharing and citation

https://writinghouse.org – Automatic bibliography and citation manager for citing pages in MLA, APA, Chicago, or Harvard

https://www.refseek.com – Academic search engine

Follow us on Twitter for our "resource of the day", or visit our Free Open Source Intelligence Resources page to see more resources like these.

More Online Training

Open Source Intelligence for Financial Investigators
40-Hour E-Learning Program

Essential for all financial institutions and corporations required to comply with the *European Union Fourth Anti-Money Laundering (AML) Directive* and similar legislation, or otherwise engaging in enhanced due diligence activities, this comprehensive training provides financial and business professionals with the latest tools and techniques required to effectively gather online OSINT, with the aim of enhancing compliance activities and minimizing potentially detrimental risks to an organization — both quickly and accurately. **Sign up or learn more** here.

This course was tremendously beneficial and relevant. It provided me with a robust set of skills to assist our member countries in fighting all types of illegal and criminal activities, including fraud, tax evasion, handling of stolen goods, corruption, money laundering, document falsification, and more. – Paulo Alves

---

Introduction to Intelligence Analysis
40-Hour E-Learning Program

This program provides a rich and interesting opportunity to explore the key concepts and intellectual foundations which inform intelligence analysis activity. Students will develop awareness of, and experience in, using common tools and methodologies to conduct analysis assignments, as well as learn how to fashion one's insights and ideas in a way that communicates effectively to clients and other intelligence consumers. **Sign up or learn more** here.

Criminal Intelligence Analysis
40-Hour E-Learning Program

This program is designed to equip aspiring and inexperienced analysts, as well as other interested law enforcement and investigative professionals, with the knowledge and skills required to undertake criminal intelligence analysis work, and to understand criminal intelligence analysis products when encountered. **Sign up or learn more** here.

40-Hour E-Learning Program

This program is intended for professionals working in public sector enforcement, intelligence, national security, and regulatory compliance roles, or those aspiring to do so. Students will be equipped with the skills and knowledge required to effectively conceive, plan, and implement strategic analysis projects, and deliver impactful strategic advice to clients and other end users. **Sign up or learn more** here.

"How-Tos" and Articles of Interest for the OSINT Professional

"4 Ways to Read Deleted Reddit Comments"

"How to Make Your Instagram More Private: 8 Useful Tips"

"Has that website been pwned? Firefox Monitor will tell you"

"Popular Dark Web hosting provider got hacked, 6,500 sites down"

"How to Stop Apps From Tracking Your Location"

"Is that fancy smart gadget a privacy nightmare? A new guide has answers."

"The 15 Best Web Proxies for Geo-Blocked Content and Online Privacy"

"How to Use a Fake IP Address and Mask Yourself Online"

"This incredibly simple privacy app helps protect your phone from snoops with one click"

"What You Need to Know About 'Dark Patterns' and How They Trick Users"

"How to Find Out When a Webpage Was Published"

"What Are Facebook Shadow Profiles? And Do You Have One"

Intel Analysis: A new study has examined why people struggle to solve statistical problems and why we seem to prefer complicated solutions over simple ones. Turns out our fixed mindsets, and our tendency to stick with familiar methodologies are to blame.

Apple CEO Tim Cook praises the EU's General Data Protection Regulations and calls for similar data protection laws in the US. Referring to the misuse of "deeply

Scientists recently analyzed language from Facebook postings to predict future diagnoses of depression and say the techniques they developed could lead to tools that could identify people in need of mental health support and formal diagnosis.

"How The Wall Street Journal is preparing its journalists to detect deepfakes"

"How to Use a Fake IP Address and Mask Yourself Online"

Follow us on Twitter for daily articles and other interesting industry updates.