Detecting Cybersecurity Threats from Online Digital Piracy Websites

Randall Suwa;
University of Hawaii: West Oahu,

Abstract

There are many threats that when using digital piracy websites that include the hidden danger of malware or downloadable files. Antivirus software may be able to identify and remove most malware, depending on how well it performs, but there are also online tools that can detect and verify the dangers associated with digital piracy websites.
This study evaluated multiple online dynamic URL analysis tools to determine the accuracy of the tools to detect the possible existence of malware from known digital piracy websites. This study seeks to verify that the presence of malware can be detected using the URL alone.

Introduction & Research Question

Introduction
Digital Piracy is a problem for many businesses that have their products illegally distributed. Many people are unaware of the possibility of a hidden malicious software in downloaded files. URL analysis tools analyze the URL or the components of the website to determine if a URL is benign or malicious. By verifying the existence of malicious intent on the digital piracy websites, this study seeks to raise awareness of these dangers and dissuade users from frequenting these sites.

Research Question
How well do online URL analysis tools perform at detecting malicious intent on digital piracy websites.

Hypothesis
There is malicious software present on digital piracy websites and that an online URL analysis tool can accurately detect the malicious intent of these websites.

Research Design & Data Collection

This study used a desktop computer running the latest version of Microsoft Windows 10 with the latest security updates. The latest version of the web browser Google Chrome was used to perform the evaluation of the URL analysis tools VirusTotal, MetaDefender, and Hybrid-Analysis. The Google search engine was used to identify potential digital piracy websites.

Data was collected by submitting the URL of the digital piracy websites to the three online URL analysis tools and the results were recorded for each of the five websites.

Results

URL for Pirate Bay reported the site was clean by all three URL analysis tools although a VirusTotal scanning engines found it suspicious but not enough to change the rating.
URL for YTS.mx reported the site was clean for all except Hybrid-Analysis which detected malicious intent from the URL.
URL for 1137x reported the site was clean although Hybrid-Analysis found the site to be suspicious.

The previous URLs were for torrenting websites. The next two are video streaming sites that host pirated content.

URL for 123Movie reported the site was clean although Hybrid-Analysis found the site to be suspicious.
URL for Putlocker was found to have malicious intent except by MetaDefender which reported the site was clean.

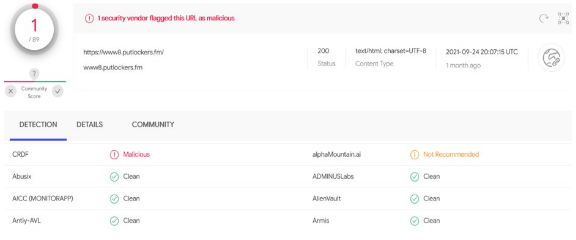
See Table 1.

Table 1. Label in 24pt Calibri.

	Pirate Bay	YTS.mx	1137x	123Movie	Putlocker
VirusTotal	o	o	o	o	x
MetaDefender	o	o	o	o	o
Hybrid-Analysis	o	x	-	-	x

Table legend: o=clean, x=malicious, -=suspicious

Figure 1



1 / 89

1 security vendor flagged this URL as malicious

https://www8.putlockers.fm/
www8.putlockers.fm

200 Status | text/html; charset=UTF-8 Content Type | 2021-09-24 20:07:15 UTC 1 month ago

CRDF	Malicious	alphaMountain.ai	Not Recommended
Abusix	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Armis	Clean

Figure 1. Label in 24pt Calibri.

Discussion

The results determined that the three online URL analysis tools reported that most of the websites clean although Hybrid-Analysis did categorize several websites malicious, and one site was identified as malicious by VirusTotal. MetaDefender determined all the sites to be clean since it used six scanning engines compared to VirusTotal's eighty plus engines and Hybrid-Defender's Falcon Sandbox. The URLs of the piracy websites may have been deemed clean due to how torrenting works from a peer-to-peer environment. Files would not be able to be identified as malicious until downloaded and scanned. The illegal streaming sites like Putlocker attempted to redirect the user multiple times to an external website which may have been why VirusTotal and Hybrid-Analysis reported the site malicious. The URL analysis tools include a file analysis tool that could used to investigate further but requires the user to download the potentially malicious file.

Conclusions

This study was unable to determine the accuracy of the URL analysis tools and whether digital piracy websites did indeed have some malicious intent. The tools determined malicious intent through reputation of the site and the URL and its components. Malware was not able to be accurately detected due to limitations of the tools and the nature of the websites themselves. Further study is required to determine a more reliable method of detecting possible malware on piracy websites.

.

Contact

Randall Suwa
University of Hawaii: West Oahu
Email: rsuwa@hawaii.edu

References

1. Alwaghid, A. F., & Sarkar, N. I. (2020). Exploring malware behavior of webpages using machine learning technique: An empirical study. Electronics (Basel), 9(6), 1–20. https://doi.org/10.3390/electronics9061033
2. Chaudhry, P. E. (2017). The looming shadow of illicit trade on the internet. Business Horizons,60(1), 77–89. https://doi.org/10.1016/j.bushor.2016.09.002
3. Hsu, F.-H., Lee, C.-H., Luo, T., Chang, T.-C., & Wu, M.-H. (2019). A cloud-based real-time mechanism to protect end hosts against malware. Applied Sciences, 9(18), 3748–. https://doi.org/10.3390/app9183748
4. Kumi, S., Lim, C., & Lee, S.-G. (2021). Malicious url detection based on associative classification. Entropy (Basel, Switzerland), 23(2), 1–12. https://doi.org/10.3390/e23020182
5. Menéndez, H. D., Clark, D., & Barr, E. T. (2021). Getting ahead of the arms race: Hothousing the coevolution of virustotal with a packer. Entropy (Basel, Switzerland), 23(4), 395–. https://doi.org/10.3390/e23040395
6. Mezzour, G., Carley, K. M., & Carley, L. R. (2015, April). An empirical study of global malware encounters. In Proceedings of the 2015 Symposium and Bootcamp on the Science of Security (pp. 1-11).
7. Moshirnia, A. V. (2018). Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat. Indiana Law Journal (Bloomington), 93(4), 975–.
8. Selvaganapathy, S., Nivaashini, M., & Natarajan, H. (2018). Deep belief network based detection and categorization of malicious URLs. Information Security Journal., 27(3), 145–161. https://doi.org/10.1080/19393555.2018.1456577
9. Sudler, H. (2013). Effectiveness of anti-piracy technology: Finding appropriate solutions for evolving online piracy. Business Horizons, 56(2), 149–157. https://doi.org/10.1016/j.bushor.2012.11.001
10. Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-turjman, F., & Mostarda, L. (2019). Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach. IEEE Access, 7, 124379–124389. https://doi.org/10.1109/ACCESS.2019.2937347