March 2017
Feature Articles: Copyright and fair use/ Should TalkTalk block Teamviewer?

ENJOY SAFER TECHNOLOGY™

Table of Contents

Copyright and Fair Use

By David Harley, ESET Senior Research Fellow

Here's a query I got recently about an article of mine from a couple of years ago on Copyright and social media: "I wanted to know that whether putting quotes of motivational speakers on social media comes under copyright? My social media network is non-profit and it is a religious network."

Here is my fairly brief response.

I'm not a lawyer and can't speak authoritatively on legal issues, but I hope these thoughts are of use to you.

Where the material you want to use is copyrighted, I think that such quotes would generally come under the 'fair use' umbrella. While this article - https://en.wikipedia.org/wiki/Fair_use - summarizes the issues as addressed by US law, it doesn't necessarily reflect practice in other jurisdictions. And even in the US, there is no absolute measurement as to what percentage of quoted material is 'fair use'.

I'm not aware of any legal framework where the religious, non-profit, or charitable status of the person or organization quoting - or indeed of the copyright holder - overrides the rights of the copyright holder.

There are also sites that actually forbid others to publish extracts from their copyrighted material. I don't know how legally enforceable that is: it may vary according to region.

As far as WeLiveSecurity and many other sites are concerned, quoting from articles in line with 'fair use' principles is fine as long as the source is acknowledged.

And here's a slightly edited version of the rather lengthier content on what actually constitutes 'fair use' that was included in that article. It's certainly not authoritative, but if you're confused about the issue, it might be useful as a starting point.

Generally speaking, simply copying copyrighted material is not ‘fair use’. Some of the most common grounds for establishing what *is* ‘fair use’ may include:

- Inclusion of quotes in a news report that summarizes a press release, article, presentation or other source. Since copyright in articles and papers generally protects the way in which they’re expressed rather than the underlying ideas, summarizing an article is, within reason, okay (plagiarizing ideas is a different issue).
- Inclusion of short passages in academic or technical articles and papers is normally acceptable, for example from other articles that support the writer’s hypothesis or provide further illustration and information regarding points made. In some circumstances, there may be issues arising from the inclusion of unpublished material.
- Inclusion of quoted material for purposes of commentary, review or criticism.
- If you’re using copyrighted material in a work that will be in direct competition with the material you’re borrowing, that’s unlikely to be considered ‘fair use’.

It's easier to plead fair use where there is no commercial advantage to the copier, but as YouTube makes clear, non-commercial use is not automatically 'fair' (and nor does giving the creator credit). There may also be grounds for pleading 'fair use' where the information disclosed is in the public interest, even in a commercial context, but again there is no guarantee.

Copyright, Plagiarism and Fair Use

Reproducing copyrighted material without authorization and passing it off as your own without credit to the real author is plagiarism. But reproducing copyright material while acknowledging the author, while it isn't plagiarism, is not in itself fair use: if it doesn't meet the fair use criteria and you aren't authorized to reproduce it, it's probably a breach of copyright. And adding a note saying that you don't intend to infringe copyright doesn't help your case if you have, in fact, infringed copyright, any more than not intending to exceed a speed limit excuses you when you *are* caught speeding. (Your excuse *might* be accepted in either case, but it doesn't mean you haven't done something you shouldn't.) Nor does a note saying that you're reproducing material for non-profit and/or educational purposes, necessarily, though if you really are, that may tip the balance towards 'fair use' where there is a dispute.
According to the 1976 Copyright Act in the US, 'fair use' can be justified on the grounds of criticism, comment, news reporting, teaching, scholarship or research, considering factors including whether it's used for commercial or for non-profit educational purpose; the nature of the work itself; how much of the copyrighted work has been re-used and how 'substantially' it represents the copyrighted content; and how the new content affects the value and marketability of the copyrighted work. (For instance, you can't reproduce substantial portions of a work with the intention of having your work supersede it.)

In Brief

- 'Fair use' or 'fair dealing' does offer limited rights to 3rd parties to make use of copyrighted material. For instance:
    - The inclusion of quotes or short passages in a news report, a technical article, or an academic paper.
    - Inclusion of quoted material for purposes of commentary, review or criticism.
    - Parody
- There is no convenient formula for estimating how much quoted material constitutes fair use. Less is definitely safer.
- Non-commercial use is not automatically 'fair use'.
- Passing off someone else's work as your own is plagiarism. However, giving credit to the author is not enough to establish 'fair use' if you don't have permission to use it.

Should TalkTalk block TeamViewer?

David Harley, ESET Senior Research Fellow
This article previously appeared on the AVIEN blog site.

It's hardly a secret that TalkTalk has had problems with tech support scams. Or at any rate its customers have, leading to suspicions that some of the scammers "… know more about their intended victims (and their issues with TalkTalk) than they should." I don't suppose for a moment that TalkTalk is actively cooperating with known scammers, of course, but it was widely reported last year that three call-centre workers at Wipro, to which TalkTalk outsourced some support services in 2011, had been arrested on suspicion of – according to the BBC – selling TalkTalk customer data.

The BBC's recent report also asserts that TalkTalk customers are targeted by "an industrial-scale fraud network in India". Commentary from Sophos hints that the issue is 'related not to TalkTalk but to one of its subcontractors'. TalkTalk has set up a site in cooperation with Get Safe Online called Beat The Scammers, which it describes as "an education and awareness campaign … designed to help you protect yourself from the growing threat of scams". The site does seem to offer some reasonable advice and offer a certain amount of insight into how these particular scammers appear to be operating, though it seems focused on old-school cold-calling rather than on pop-ups directing victims to 'helplines'. Still, most of the old tricks are still used by 'next-generation' scammers. And in fact, I quite like the idea of 'The Nevers', a short list of things that a TalkTalk representative 'will never do'. For instance:

- Ask for a customer's full password (apparently they may ask for two digits)
- Ask for bank details to process a refund (details the company should already have)
- Ask the customer to send money through services like MoneyGram or Western Union (two services very commonly used by scammers)

However, the company has also upset some of its customers, according to Kat Hall (writing for The Register), by blocking TeamViewer, a remote access/desktop management tool – TalkTalk blocks TeamViewer – Wants to protect customers from phishing and scamming.

It's perfectly true that TeamViewer, like AMMYY and several similar tools/sites, is widely used by support scammers. But it's a legitimate service also widely used for entirely legitimate desktop management purposes. A blanket ban on its use is rather like an anti-malware application deciding to make it impossible for a customer to run 'Possibly Unwanted' or 'Possibly Unsafe' applications. We don't do that – well, most of us don't – because although it might make some customers safer, some people would be seriously inconvenienced by it. Apart from the fact that those people would have to take their business elsewhere, it hardly seems appropriate for a security company to deny its customers access to legitimate services. There is a classic tripod model of security, said to consist of Confidentiality, Integrity, and Availability. Take away availability, and what you have is no longer security.

ESET Corporate News

New Additions to ESET Remote Administrator and ESET Virtualization Security

ESET has introduced two major compatibility updates for its endpoint security solutions. Focusing on expanding protection for enterprise customers, ESET Remote Administrator is now compatible with IBM QRadar, a security information and event management tool for collecting and analyzing security log data. In addition, ESET Virtualization Security now includes native support for VMware NSX, further growing ESET's solutions for the popular VMware platform.

While cyberattacks continue to escalate in frequency, severity and impact, most organizations tend to stagnate with improvements in infrastructure. Organizations that successfully establish an ecosystem that balances protecting and growing the business will remain competitive and in a position to address cybersecurity threats.

ESET Remote Administrator is designed to enable IT staff to oversee the entire network, from a single point. With the integration of IBM QRadar, companies will benefit from the flexibility of ESET Remote Administrator while taking advantage of IBM's core competency in infrastructure deployment. Major improvements include:

· **IBM QRadar Integration:** All major ESET events are exported in LEEF format, which is natively recognized by IBM QRadar. ESET Remote Administrator is shown as a "Log Source" in the IBM QRadar console.

· **Multi-tenancy:** Ideal for large enterprises with one centralized server and different admins managing only endpoints in their respective locations, or for MSPs managing multiple customers from a single server but who need to ensure that customers are not able to see the data of other users.

· **iOS Mobile Device Management:** Integrated directly into ESET Remote Administrator, now supports Apple Device Enrollment Program and offers extended functionalities of app white/black listing, web filtering, device security settings and notifications, anti-theft and others.

ESET Virtualization Security is a VMware, vShield-based solution that allows offloading of AV scanning to a central machine. Paired with ESET Remote Administrator 6, it allows for simple management, automation and control over all protected computers / devices on the network, including physical desktops, servers and virtual machines.

· **Native support for VMware NSX automation:** ESET Virtualization Security natively supports micro-segmentation and automatic task execution that automatically moves infected machines to a different micro-segment, to prevent the spread of malware, and executes scanning. Automatic deployment of ESET Virtualization Security appliances to hosts newly connected to NSX Manager allows instant protection of newly added virtual hosts and virtualized workloads.

· **Easy to deploy:** As soon as ESET Remote Administrator is installed, ESET Virtualization Security appliances can be deployed on multiple hosts at once.

· **Superior performance:** VM infrastructure is about optimizing resources and performance, and ESET's scanning engine exactly meets these requirements. It is well-known for its low system demands and high speed, leaving more resources for other applications and processes.

To learn more about ESET Remote Administrator and other business solutions, visit eset.com.

ESET discovers fake Minecraft mods on Google Play

It wasn't long ago that Minecraft was connected to a scareware campaign that preyed on users looking for Minecraft cheats. ESET researchers have recently report another misuse of this popular app: fake Minecraft mods on Google Play are pestering Android gamers with aggressive ads and scam activity. So far players have been exposed to 87 fake mods, and up to 990,000 users have installed them.

ESET researchers have divided malicious activity connected to fake mods for Minecraft into two main categories: ad-displaying downloaders, detected by ESET as Android/TrojanDownloader.Agent.JL and fake apps redirecting users to scam websites, detected by ESET as Android/FakeApp.FG.

The full analysis of fake mods for Minecraft on Google Play is now available on WeLiveSecurity.com.

In addition to only downloading apps from the official app store, it is also recommended that users use a mobile security product like ESET Mobile Security to help detect and flag malicious activity.

The Top Ten Threats

1. Win32/TrojanDownloader.Wauchos

Previous Ranking: 1
Percentage Detected:5.62 %

This is a Trojan which tries to download other malware from the Internet. It collects information about the operating system, including configuration settings and the computer's IP address. Then, it attempts to send the information it has gathered to a remote machine. It can download files from a remote computer and/or the Internet, run executable files, create Registry entries and remove itself from the infected computer.

2. LNK/Agent.DA

Previous Ranking: 3
Percentage Detected: 3.24%

LNK/Agent.DA is a detection name for a *.lnk file that executes the Trojan Win32/Bundpil.DF. The LNK file is part of a Bundpil attack and is created with the special name "%drive_name% (%drive_size%GB).lnk" on removable drives, convincing users that it's a link to drive content. It actually points to %system32%\rundll32.exe with a Bundpil DLL component as a parameter.

3. JS/Danger.ScriptAttachment

Previous Ranking: 2
Percentage Detected: 3.02%

JS/Danger.ScriptAttachment is a generic detection of suspicious e-mail attachments.

4. Win64/TrojanDownloader.Wauchos

Previous Ranking: 5
Percentage Detected: 2.93%

This is a Trojan which tries to download other malware from the Internet. It collects information about the operating system, settings and the computer's IP address. Then, it attempts to send gathered information to a remote machine. It can download files from a remote computer and/or the Internet, run executable files, create Registry entries and remove itself from the infected computer.

5. HTML/FakeAlert

Previous Ranking: 4
Percentage Detected: 2.86%

HTML/FakeAlert is a generic detection name for an HTML page showing a made-up, fake alert message, usually about a fictional virus infection or some other problem which is supposed to harm the computer or the computer user's data. The user is usually urged to contact fake technical support hotlines or download and execute a fake security solution from the Internet to prevent "damage". This kind of page is usually used as a starting point for 'Support Scams'.

6. Win32/Adware.ELEX

Previous Ranking: 10
Percentage Detected: 2.53%

Win32/Adware.ELEX is an application designed for delivery of unsolicited advertisements to an affected computer. Usually, it alters the behavior (settings) of an Internet browser (for example adware sets its own "homepage" and setting back this value to original value is no easy task - the adware or a component of the adware is protecting this setting). Then the adware displays small windows with advertisements within the browser.

7. Win32/Bundpil

Previous Ranking: 7
Percentage Detected: 2.37%

Win32/Bundpil is a worm that spreads via removable media. The worm contains a URL from which it tries to download several files. The files are then executed and HTTP is used for communication with the command and control server (C&C) to receive new commands. The worm may delete files with the following filename extensions:

*.exe

*.vbs

*.pif

*.cmd

*Backup

8. HTML/ScrInject

Previous Ranking: N/A
Percentage Detected: 1.51%

HTML/ScrInject is a detection of program code that redirects the browser to a specific URL location with malicious software. The program code of the malware is usually embedded in HTML pages.

9. HTML/Refresh

Previous Ranking: 9
Percentage Detected: 1.39 %

HTML/Refresh is a Trojan that redirects the browser to a specific URL serving malicious software. The malicious program code is usually embedded in HTML pages.

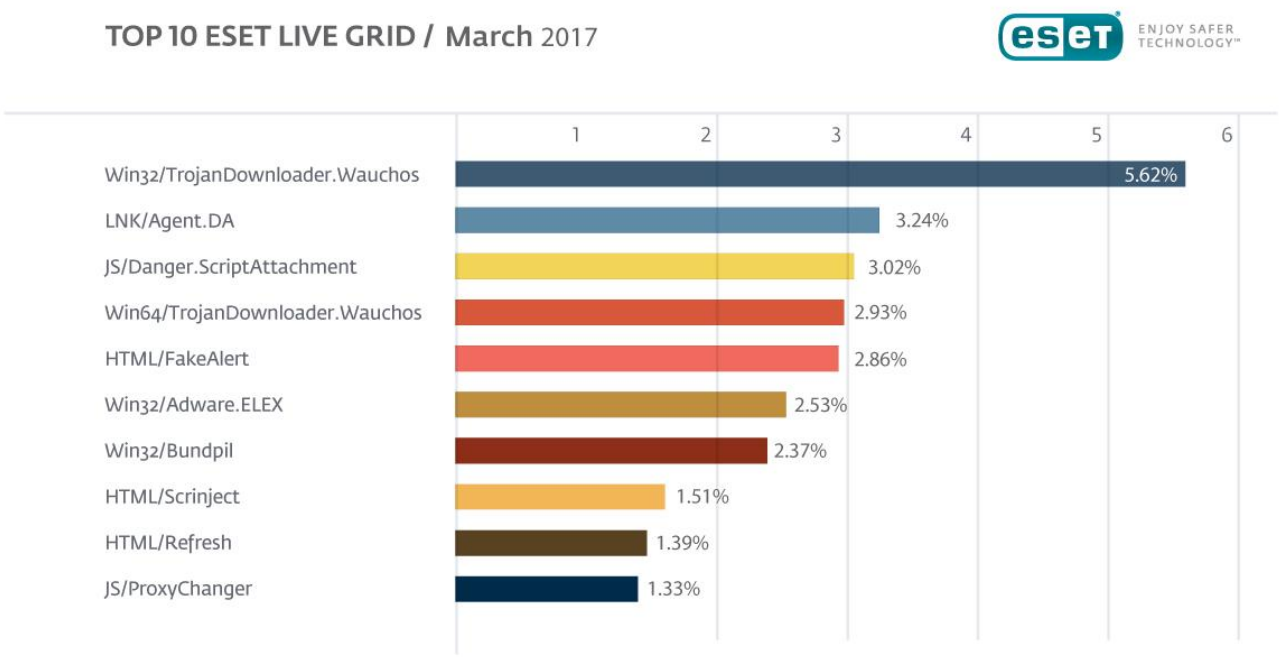
10. JS/ProxyChanger

Previous Ranking: 6
Percentage Detected: 1.33%

JS/ProxyChanger is a Trojan that prevents access to certain web sites and reroutes traffic to certain IP addresses.

Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with 5.62% of the total, was scored by Win32/TrojanDownloader.Wauchos.



About ESET

For 30 years, ESET® has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real-time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn 100 Virus Bulletin VB100 awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information visit www.eset.com or follow us on LinkedIn, Facebook and Twitter.

More information is available via About ESET and Press Center.

Additional Resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources, please visit:

- VirusRadar
- ESET White Papers
- ESET Conference Papers
- WeLiveSecurity
- ESET Podcasts
- ESET Videos
- Case Studies