==Phrack Inc.==

Volume 0x10, Issue 0x46, Phile #0x0f of 0x0f

```
|=-----------------------------------------------------------------------=|
|=---------------------=[ YouTube Security Scene ]=----------------------=|
|=-----------------------------------------------------------------------=|
|=--------------------------=[ LiveOverflow ]=---------------------------=|
|=-----------------------------------------------------------------------=|
```

--[Table of Contents

--[0. About the Author

To briefly introduce myself, I'm LiveOverflow and I make videos about various IT security topics. Here are a few:

+ How SUDO on Linux was HACKED! // CVE-2021-3156
    https://youtu.be/TLa2VqcGGEQ?list=PLhixgUqwRTjy0gMuT4C3bmjeZjuNQyqdx
+ XSS on Google Search - Sanitizing HTML in The Client?
    https://www.youtube.com/watch?v=lG7U3fuNw3A
+ Identify Bootloader main() and find Button Press Handler
    https://youtu.be/yJbnsMKkRUs?list=PLhixgUqwRTjyLgF4x-ZLVFL-CRTCrUo03

--[1. Preamble

From BBS and text files, over IRC and books, to the modern internet with forums and blogs, hackers exchanged information primarily in text form. This of course meant, most older hackers prefer text, which makes it difficult to establish new kinds of media.

When I started producing videos in 2015 I often got the feedback that text is superior, nobody will watch videos and I should instead write articles. So when I was asked to write about the "YouTube Hacking Scene" for Phrack I felt like video production finally reached some level of acceptance.

While this article is titled "YouTube Hacking Scene" I also want to include streamers on Twitch and other platforms - who knows how long the product YouTube will survive, and I'm sure Phrack will exist long after.

Given that my personal experience is biased and the history is difficult to research, this article is certainly not objective. So we will go with the French saying "preach the falsehood to know the truth". So if you know it better, please reach out.

--[2. Before 2014

Digging up information about hacking videos from the early 2000s is difficult, but it's clear that it was not very popular. Personally I remember "Lenas Reversing for Newbies"[0] video series from 2006 very well, but it wasn't distributed via YouTube. It is an incredibly detailed and hands-on walkthrough of Windows reverse engineering and cracking with OllyDbg. I have seen it getting recommended a lot over years, indicating that there is a craving for the visual teaching approach.

One of the earliest hacking show attempts seems to be "the broken" by

Kevin Rose from 2003[1]. Then in 2005 Darren Kitchen started the Hak5 show[2] and it deserves a mention, as it is probably the longest running hacking video production. YouTube already existed when it started, but it wasn't popular just yet, so the distribution heavily relied on torrents. Notable might also be IronGeek, who started uploading conference videos on YouTube in 2007. His trip to Notacon 2007 might be the first ever "Hacking Vlog"[3]. But all of these video projects were mostly just scratching the surface of hacking. Very few videos were actually digging into the technical details.

In 2007 the project SecurityTube started out of India by vivekramac. Probably inspired by YouTube it was meant as a place for everybody to upload and share hacking video content, but vivekramac himself was responsible for creating tons of videos. For many years it seems to have been the best source for free video courses. But in 2011 the site slowly transitioned into the new paid courses platform Pentester Academy.
Fun fact, when I started making videos in 2015 I obviously came across SecurityTube and I tried to submit my videos there, but they were never accepted. The platform already felt abandoned, and the content was kinda outdated and not the depth I was looking for anyway. Nonetheless a very important part of video creator history.

Over the years I have been collecting YouTube channels with more or less technical security content. And to create the chart below (Fig. 1), I looked at the year of their first relevant upload. Also most of those channels only have a handful of videos and were abandoned shortly after. But in hindsight I even noticed there were a few very early attempts at making more technical video walkthroughs such as lordparody (2009)[4]. Looking at the data there appears to have been a small surge after 2010, but I think that 2015 was where the current hacker creator scene really started growing.

```
        2005: *
        2006:
        2007: **
        2008: *
        2009: *****
        2010: ****
        2011: *******
        2012: ************
        2013: *********
        2014: ******
        2015: ***************
        2016: **************************
        2017: ****************************
        2018: *********************
        2019: ************
        2020: *********************
```

Fig 1. Bar chart showing the numbers of
new hacking YouTube creators by year

--[3. My Start in 2015

Around 2014 I started to hit a wall in my own learning progress. There were tons of (written) tutorials about web security, WiFi hacking, Metasploit and buffer overflows, but the material mostly covered basics. To actually learn more advanced topics I had to play wargames[6] and CTFs. I remember fondly struggling for months playing w3challs or io.smashthestack to improve very very slowly - I was a classic annoying noob, even getting banned by bla from IRC ;)

I believe it shouldn't have been this difficult to progress. In the traditional academic science community you rely on papers, to build upon prior research. And while we have equivalent resources, see for example Phrack, we are missing the educational institutions like universities to pass on this knowledge more effectively. So in the past, new people had to walk a very stony path to catch up with the state-of-the-art. After I finally "understood" ret2libc and ROP, I felt like that this stuff is actually easy, but the existing material is just bad at explaining it.

Then in late 2014, early 2015, two events happened that would have a big impact on me. The first event was the growing community of programmers on reddit called /r/WatchPeopleCode[7] - a subreddit about live streaming programming. While it is not about security, everybody knows that programming skills are crucial if you do any form of more in-depth hacking. The second event was geohot livestreaming himself solving pwnable challenges from overthewire.org[8].

What both of these events have in common is that it's the first time for me looking over the shoulder of a professional. I realized that all the talks, blog posts and articles only cover the results, and rarely the actual process. And because I was not lucky enough to have people around me to learn from in person, watching over the shoulder of an experienced developer, or geohot, was eye opening.

To see how geohot was using the terminal, writing exploit scripts and navigating IDA Pro was incredibly insightful. But more importantly, it also exposed the fails and mistakes followed by the process of troubleshooting and fixing the bugs. And this pushed me through the wall I was hitting in my own education.

I was craving more. Where can I find more streams or videos where people are hacking? Unfortunately, when searching on YouTube, the only videos I could find were either Metasploit tutorials or how to use aircrack-ng to hack a WiFi. And these topics were very boring to me as I was more interested in the process of finding these kinds of flaws, rather than just using what others found.

Of course I was very far away from geohot's skills, I did understand ROP and I thought I could create the "over the shoulder" experience for the people coming after me. Which led me to start livestreaming pwnable challenges[9] from exploit-exercises.com (today exploit.education), and cover other CTFs. However I quickly noticed that I was terrible at streaming and soon transitioned into making scripted videos with a focus on visual explanations[10]. Another realization I had was, in fact, I did not understand ROP and other topics properly. So having the aspiration to create better tutorials, it forced me to dig deeper, which meant this project benefited my own education too.

Of course this is me talking from my own perspective and I don't want to make it sound like I was the only one. I simply wanted to provide insight on what motivations can lead people to create videos. So at this point I would like to mention a few other folks who were making videos about more "advanced" topics around that time. Gynvael from the Dragon Sector CTF team[11], MurmusCTF[12], ipp[13], psifertex[14], Zeta Two[15] and probably many more I unfortunately never came across.

Making good videos is very time consuming, especially once it's more than "just" a screen recording or livestream. So very few creators are able to do it over a longer period of time and I believe John Hammond[16] and I have the longest and consistently running release schedule.

--[4. Today's Scene

As has been the case with any area of hacking, commercialization also creeps into this scene. I'm not immune to this either, as the time investment is massive and has to be justified somehow. This unfortunately leads to videos that are sometimes more motivated by exposure or products, rather than the pure sharing of knowledge; and it's difficult to find a balance between those opposing forces. It also led to the prior generation of free video content (SecurityTube, Cybrary, ...) to put their content behind paywalls.

But there is one amazing positive commercial development that I want to highlight. In the past years companies like Google have sponsored very technical videos[17] to share insights into vulnerabilities of their own products. Who would have thought this could ever happen, when this community used to be scared to get sued for anything.

There are also new problems that come with Google/YouTube and the other large social media platforms. YouTube for example has a policy against certain kinds of hacking videos[18], which lead to the take down of several videos and even entire channels. However it should also be noted 99% of the time it was a clear mistake and the decisions got reversed.

> "Hacking: Demonstrating how to use computers or information technology with the intent to steal credentials, compromise personal data or cause serious harm to others such as (but not limited to) hacking into social media accounts."
> - YouTube's harmful or dangerous content policies

Can hacking videos be ethical or unethical? It's a difficult topic and one that I clash a lot on with other creators. I do believe that there is a way to make the "right" kind of tutorials - and so far I haven't had any issues with YouTube ;)

For example, I understand that Google does not want a step-by-step video guide for script kiddies to setup a shitty phishing page, when phishing is the second most common source of compromised Google accounts[19]. And to me that is not censorship, because the underlying skill is very basic web development. So to me a phishing tutorial is kinda deceitful and unnecessarily hiding the real "hacking" skill - web development. But I know many of my peers disagree here.

Then there is the evolution of "hacker influencer". It was important to me at the start to be faceless anonymous. But over the years my opinion has slightly changed. I often think back to the time when I was sitting alone in my room trying to understand an article, and wished I had the videos I make today. So for me it's important to use social media and their algorithmic feeds to maximize exposure; hoping to reach that kid who wants to break through the same wall I was hitting. Nowadays I believe that my desire to have this information easily discoverable, outweighs restricting educational resources to obscure (or underground) places.

In 2019 TheCyberMentor joined the scene with live streaming basic pentesting lessons for free on Twitch[20]. It kinda felt like OSCP material, just in video form and free. There were earlier attempts at creating free pentesting courses, such as SecurityTube or Cybrary, and maybe others as well. But TheCyberMentor is undoubtedly the most successful one, reaching several millions of views. This hasn't lasted long though, since building up the initial audience, he transitioned away into paid courses too.

There is also some criticism regarding original content vs. taking existing (written) tutorials and turning them into videos. Certainly there is added value in improved presentation. But there is also the ethical question about highlighting the sources. This especially affects newcomers where sometimes it's obvious that they follow a typical outline from other material, without referencing it.

In the past years, there has also been an interesting development about topics covered by the video creator scene. Because it has been completely dominated by "bug bounties". As much as I love seeing an influx of motivated young people, it feels like this is our community's version of the "get rich quick" scam. It leads to a huge demand for paid courses and guides that directly or indirectly promise you to make you a successful bug hunter. Currently it's very rare to see content beyond bug bounties and I wish there was more diversity.

Sometimes I also think about how hacking communities organize, and how creators changed this. In the past the communities were usually divided by topics of interest, and now the communities form around personalities. Sometimes this makes me a bit uncomfortable, but this also resulted in a massive increase in exposure to the hacking world (it benefits the creator when the fan base grows).

It's always difficult to see cultural change, when it evolves away from what we grew up with. But thinking back to my teenage years, I wish I could have been able to find places like that more easily, instead of having to wait until my 20s to accidentally stumble into it.

Besides creating videos, there is also a growing scene live streaming on Twitch. Most of them work on challenges from HackTheBox or TryHackMe, which are platforms with commercial interest. This means the streamers provide collectively free advertising worth millions for those platforms. On one hand it's amazing to see so much content, but it's sad that less community oriented wargames/CTFs are shown. And the variety of the topics covered is very low as well.

The style (screen recordings vs. person talking vs. heavy editing), and the skill levels of creators vary a lot. And I don't mind, as variety benefits us all. I'm happy as long as more people share more of their work in video form. I even would like to see more beginners documenting their journey. But deep down my heart beats for the senior professionals, like geohot at the time, who let us look over their shoulder.

And there are some great channels today, such as hardware researcher stacksmashing[21], gamozo who develops entire new operating systems just for fuzzing[22] (absolutely insane) or the Flashback Team diving into their Pwn2Own winning router hack[23]; those kinds of channels make me excited.

The popularity of hacking videos, and the evolution of a whole creator scene, was only possible due to the growth of social media platforms. Their algorithms helped us to get our videos in front of people who didn't know they were looking for them. As the internet changes fast, social media platforms change too, And right now TikTok seems to be an interesting platform to reach new audiences, but the short format does not allow to cover in-depth topics. MalwareTech[24] is leading the charge there with millions of views.

--[4. Final Words

Unfortunately there are so many creators today that I cannot include everyone. But please know that this article is dedicated to all of you.

The following people have helped me with this article, by sharing their experience or fact checking information (alphabetical order):

BlindHacker, CryptoCat, gamozo, Gynvael, hacksplained, insiderphd, ipp, John Hammond, justinsteven, Murmurs, psifertex, snubs, stacksmashing, superhero1, TheColonial, Zeta Two

Shoutout to the polish and indian video creators. I do not understand a single word, but you all seem very active and dedicated. Special shoutout to geohot, because without his CTF live streams I would not be here. And shoutout to Gynvael for being the first person I really cared about acknowledging my work.

"And don't forget to like, comment and subscribe."

--[5. References

[0] Lenas Reversing for Newbies (2006) https://web.archive.org/web/20070524043123/http://www.tuts4you.com/download.php?list.17
[1] thebroken by Kevin Rose https://archive.org/details/thebroken_xvid
[2] Hak5 - Episode #1 https://www.youtube.com/watch?v=SUEXCCWMfXg
[3] Notacon 2007 Part 1 https://www.youtube.com/watch?v=HXSZ4PRLUDU
[4] CSAW CTF challenge 2.exe, 3.exe and 4.exe flag retrieval https://www.youtube.com/watch?v=_Ld1cD9d7tI
[5] Beginner Challenge #1... https://www.youtube.com/watch?v=tdqJ8NEcJUM
[6] Phrack issue #69 - International scenes

```
 [7] https://reddit.com/r/WatchPeopleCode
 [8] livectf REDEMPTION by geohot 7/27/2014
     https://www.youtube.com/watch?v=td1KEUhlSuk
 [9] Let's Hack Livestream - exploit-exercises.com (2015)
    https://www.youtube.com/watch?v=HBnPY77JtqY
[10] The Heap: dlmalloc unlink() exploit - bin 0x18
     https://www.youtube.com/watch?v=HWhzH--89UQ
[11] Hacking Livestream #1: ReRe and EZPZP
     https://www.youtube.com/watch?v=XWozhb1ZOyM
[12] Life of an Exploit: Fuzzing PDFCrack with AFL for 0days
     https://www.youtube.com/watch?v=8VLNPIIgKbQ
[13] HackTheBox - Popcorn https://www.youtube.com/watch?v=NMGsnPSm8iw
[14] Live CTF v2: ... https://www.youtube.com/watch?v=D7uXE_lEzxI
[15] SMT in reverse engineering, for dummies https://youtu.be/b92CW-NZ3l0
[16] GoogleCTF - XSS "Pasteurize" https://youtu.be/voO6wu_58Ew
[17] Hacking into Google's Network for $133337 https://youtu.be/g-JgA1hvJzA
[18] https://support.google.com/youtube/answer/2801964?hl=en
[19] Data breaches, phishing, or malware? Understanding the risks of
     stolen credentials https://dl.acm.org/doi/abs/10.1145/3133956.3134067
[20] Zero to Hero Pentesting
     https://youtu.be/qlK174d_uu8?list=PLLKT__MCUeiwBa7d7F_vN1GUwz_2TmVQj
[21] How the Apple AirTags were hacked https://youtu.be/_E0PWQvW-14
[22] FuzzOS: Day 1, starting the OS https://youtu.be/2YAgDJTs9So
[23] How We Hacked a TP-Link Router and Took Home $55,000 in Pwn2Own
     https://www.youtube.com/watch?v=zjafMP7EgEA
[24] https://www.tiktok.com/@malwaretech
```

```
|=[ EOF ]=---------------------------------------------------------------=|
```