Steam

Beloved gaming client and security tale of woe: A history

Lahna “Fury” Sheron
12/9/17

CONTENTS

ABSTRACT

If you play videogames, chances are you know about Steam, the gaming platform, software distributor, digital rights manager, content creation forum, and social network released by Valve Corporation in 2003 that currently offers 18,242 [1] games for purchase and download. In 2016, Valve reported 125 million active lifetime users, and active monthlies were pegged at 67 million [2]. As anyone might imagine, a considerably robust security system needed to be implemented given the sheer scale of Steam and the technical nature of its consumer base. There have been several incidents over the years despite this system's development, however. This paper will discuss the illustrious history of Steam's security system, including the implementation of Steam Guard in 2011, the DDoS attack of 2015, the Steam Stealer malware incident of 2016, and the state of the system today.

INTRODUCTION

Valve as a studio had certainly gained critical and global acclaim for itself as a game developer by the time the early 2000s rolled around because of their inventive first-person classic, Half-Life, so when it was announced that Valve was going to begin offering a service free for users that allowed developers to publish their games through the cloud without needing to go through physical manufacturers or stores, it wasn't surprising that it became a standard of PC gaming quite quickly. Steam was the first platform of its kind, and in the earlier days of the internet, that was more than enough to garner a monopoly on users. It wouldn't be until much later that alternate services such as EA Origin, GOG.com, or HumbleBundle would even surface, let alone garner attention.

Once a user has a Steam account, they can link it to payment options and other social media and set it to public and private. From there, users are free to friend other users and purchase games. An important note about Steam is that it's not just used for gaming; it's a hub for the sharing and creation of content like game mods, fanart, articles, videos, game reviews, and more. What's more, any game with in-game items, cosmetic or otherwise, comes with its own economy based around buying and selling these items. These trading economies are one of the biggest mediums for attackers on Steam.

Steam does have explicit protocol regarding security issues, and has taken several measures over the years in order to protect its millions of users and evolve with the threats its technically-

minded community keeps coming up with. Valve doesn't have an active money-reward-based bug bounty, but it does offer recognition to users who report bugs [3] and releases security notes in the Steam forums after all incidents.

TO THE COMMUNITY

I chose to focus on the history of Steam, specifically, because I think it's an interesting narrative that exemplifies software that emerged early and started small that came to have a massive user base. Steam is also the biggest digital games distributor user-wise, so I thought it would be useful for those who have a Steam account to have a consolidated history of Steam's largest security mishaps and what Valve, as a company, has done in response to counteract them.

What's more, I think it's important for Steam users to be aware of all of these incidents because almost every time Steam changes, their malicious, tech-minded peers will take advantage of it. Essentially, I'd like to instill in users this most simple message: don't get to comfortable. Steam is still a digital service that deals in the exchange of currency of millions of people, and as such, it's vital that all users be aware of what they're doing with their information at all times. Steam's story isn't a unique one; it's full of the same vulnerabilities and exploits that are still being taken advantage of today across the internet.

TIMELINE

2011: Steam Guard and Breach

To begin examining the interesting part of Steam from a security perspective, I think it's prudent to cut out the first few years and jump to 2011 and the release of Steam Guard, a two-factor authentication service. Originally, the only feature of Steam Guard was requiring a user to enter a code emailed to them in order to log into an account on a non-default system. [4] That is, any system. Valve doesn't limit the amount of devices onto which you can log into your Steam account because, in their words, they think security should be about "[aiming] to protect the value that is yours, not [limiting] your access to your stuff." [5] Later that year, however, would see Steam's first large security breach. Attackers, through an undisclosed security flaw in Steam's forums, gained access to login details, and using these credentials managed to access Steam's database of usernames, passwords, game purchases, and credit card information. Fortunately, the passwords were thoroughly hashed and salted, the credit card numbers were encrypted, and as such

nobody had been robbed, but the fact that the attackers got to that database at all was a huge problem. [6] Three months later, in February of the next year, Valve released a public update about the breach, stating that the investigation team they'd hired reported that the attackers may have obtained a backup file for the period 2004-2008 containing usernames, emails, encrypted billing addresses, and encrypted credit card information, but not passwords. [7] There was some backlash among consumers about the amount of time it took Valve to release its 2012 statement and the magnitude of its contents. [8] Response time becomes a theme among backlash to Valve as a service provider. In all of its responses to this particular issue, Valve urged users to sign up for Steam Guard, as it would definitely assist in ensuring the safety of user information.

2014: ssfn* Files and Phishing

Three years was as long as it took for attackers to find a way to mess with Steam Guard. In 2014, there was a large phishing scandal involving Steam Guard, specifically. A user would click on a fake Steam page in-browser, and then a Steam Guard prompt clone would pop up (image courtesy of MalwareBytes). It would say "As an added account security measure, you'll need to grant access to this browser by uploading the special ssfn* file from your Steam folder…Ssfn* file contains your ID number and located in a directory Steam folder (…/Program Files/Steam/ssfn*)" The user would then upload their ssfn file, which incidentally doesn't contain the user's ID but rather acts as a flag for logging in with Steam Guard. In other words, a device without the ssfn file would send an email verification to a user's email address every time they tried to log into their Steam account. However, a device that *did* possess the ssfn file would believe it was cleared as the "home base" computer, and wouldn't prompt for password or Steam Guard check when a user entered their username. [9] An update of this phishing scam was released later, in the summer of that year, when the prompt stopped asking users to locate the file themselves, but rather open a "special tool" that automatically located the file and uploaded it. [10]

2015: Password Problems, Trading Restrictions, and the 2015 DDos Christmas Attack

As Steam became more and more ubiquitous as a PC gaming client, Valve started to be perceived as more of a faceless corporation rather than the loveable, small game studio that had made the Portal franchise. It became infamous for being generally unresponsive as a customer support network, but reacted quickly when it came to large-scale exploits. An interesting example came in July 2015 as an exploit in the Steam client allowed anyone to change the password on any account. An attacker would enter an account name into the "forgot my password" section of the

login screen, then get a code sent to the account's registered email. When the attacker was prompted for a code, pressing "continue" having entered nothing into the code field would advance the page, allowing the attacker to change the account's password at will with no penalty. Valve had this issue patched within 24 hours of the exploit's discovery on July 25th. [11]

Later that year, Valve buckled under the amount of fraudulent purchases from stolen accounts and began imposing time-based trading and gifting restrictions. Valve claimed that they'd been aware of the problem for two years, but had refrained from imposing restrictions on the community because they felt "the impact fraud was having on players and the economy wasn't big enough compared to the drawbacks of imposing restrictions on everyone." [12] The subsequent years would hold a shocking spike in the number of fraudulent purchases and account thefts, to the point Valve feared they may no longer be allowed to accept payment via credit card at all. In early December of 2015, Valve announced that it was seeing around 77,000 accounts hijacked per month. [13] So they implemented a system that put regional and temporal restrictions on trading and gift-giving. Users that lived in trade-restricted regions, like Russia, would only be permitted to play games they bought or were gifted in that region while they were physically there. In the event that they vacationed or emigrated, they wouldn't be able to use those games or items anymore. Valve stated, "We hated doing it, but we didn't have a better solution. We are continuously exploring different methods to solve these problems." The most apparent of these methods would be that at this point in time, Valve had developed the Steam Guard Mobile Authenticator. It added the mobile device as an extension of the Steam Guard two-factor authentication service. Instead of needing to log in to an email account to access a code, users look at their Mobile Authenticator, which generates a new random code every 30 seconds. Valve believed that this increased security measure would sufficiently protect users who enabled it from account theft, but since they didn't force users to enable it, they wanted to introduce a new feature to Steam itself to protect those who either "felt they were smart enough about security to not need two-factor authorization" or "knew they needed it, but couldn't use it due to reasons beyond their control, like not having access to a mobile phone." As such, anyone without the Mobile Authenticator would have delays of up to three days for item delivery as a result of trading.

Malware creators were quick to find a way to phish this new system. Fake domains were set up as early as December 3rd that scammed users. They would attempt a trade through the third-party site, a commonplace action, and the site would download an executable to the user's computer, stating the trade would not be completed until "Escrow" (a term used to describe the

officially titled Steam Trading Holds) was enabled and run. Sometimes this executable was a backdoor and sometimes it was a virus. [14] There's no patch that can be issued against phishing, so there wasn't much Valve could do besides attempt to shut down the sites and educate the public.

Account theft and phishing on the rise wasn't the only of Valve's problem December of 2015, however. During possibly the busiest time of any consumer-goods seller on the internet, Christmas, the Steam store was hit with a DoS attack. Valve's statement five days later read:

> *Early Christmas morning (Pacific Standard Time), the Steam Store was the target of a DoS attack which prevented the serving of store pages to users. Attacks against the Steam Store, and Steam in general, are a regular occurrence that Valve handles both directly and with the help of partner companies, and typically do not impact Steam users. During the Christmas attack, traffic to the Steam store increased 2000% over the average traffic during the Steam Sale.*
>
> *In response to this specific attack, caching rules managed by a Steam web caching partner were deployed in order to both minimize the impact on Steam Store servers and continue to route legitimate user traffic. During the second wave of this attack, a second caching configuration was deployed that incorrectly cached web traffic for authenticated users. This configuration error resulted in some users seeing Steam Store responses which were generated for other users. Incorrect Store responses varied from users seeing the front page of the Store displayed in the wrong language, to seeing the account page of another user.*
>
> *Once this error was identified, the Steam Store was shut down and a new caching configuration was deployed. The Steam Store remained down until we had reviewed all caching configurations, and we received confirmation that the latest configurations had been deployed to all partner servers and that all cached data on edge servers had been purged. [15]*

The information revealed included users' billing addresses, the last four digits of their Steam Guard phone numbers, their purchase histories, the last two digits of their credit card numbers, and their email addresses. Users who weren't on Steam at the time of the attack were unaffected.

2016: More Trading Restrictions, Community Backlash, and Purchasable Malware

After Valve gathered enough data about their new trade restrictions, concluding that they'd concretely made a dent in detecting account and item theft (at that point 95% of daily trading involved the new Steam Mobile Authenticator) they decided to make them even more severe. [16] For those who do not have the Mobile Authenticator, the trade hold period was lengthened from three days to fifteen, "to protect users who log in less frequently and who need more time to

identify a problem." Trades with a friend older than a year would be only one day, though. This security update also brought market holds, a process to protect players' inventory against more than trade fraud, where a user needed to wait an amount of time until a market posting they created went live and could be bid on. In addition, a new sort of gifting restriction was introduced; in the event that you gifted your friend a game and they got banned within it, you'd be unable to gift that game to anyone ever again. This rule was put in place to attempt to combat game hoarding.

There was massive community backlash against these further restrictions, mostly around the fact, again, that the Mobile Authenticator wasn't accessible to everyone. Anyone without an Apple or Android smartphone (a Windows Phone version of the Steam mobile app wouldn't come out for almost another 4 months) would be left in the dust and be unable to escape the lengthened trade holds.

Sadly, these new restrictions couldn't stop entirely the trend of malware that came out roughly the same time: Steam Stealers, a sellable "malware-as-a-service" a less experienced attacker would purchase from a more experienced malware creator in order to steal accounts. The Steam Stealers were cheap – according to MalwareBytes, purchasable malware usually goes for about $500 per instance, but a Steam Stealer could be found for as low as $3 and no greater than $30. Steam Stealers could take the form of fake login screens, fake websites, malicious downloadable mods, and trading holds wouldn't act as much of a deterrent if the attacker still had access to the account once the hold was lifted. [17]

2017: Cross-Site Scripting Steam Guide Profile Exploit

Early 2017, users who hadn't even succumbed to phishing were having their Steam Wallets drained and accounts tampered with. Before Valve had even patched the issue, a seasoned web developer and mod of the Steam subreddit took the time to explain the details of this incident. He explained what Cross-Site Scripting or SQL Injection were, and elaborated on how both techniques were used in this attack to target Steam's temporarily vulnerable game guide write-ups. If a user has written a guide for a game, they have the option of displaying it on their profile. Injecting some malicious JavaScript into a guide would cause any user who clicks on a legitimate link to a profile to be redirected to a non-legitimate clone of the user page. Additionally, since steam market transactions don't *require* Steam Guard, this malware could place market bids without the victim's knowledge, and would silently buy as many CS:GO "Anarchist" cards the hijacked user could

afford, all by just clicking on a legitimate profile. [18] Security firm SentinelOne's chief of security strategy claimed that these malicious scripts could have also stolen authentication cookies to automatically access accounts from browser, which would lead to self-replicating behavior. [19] The fix was easy, Valve just needed to stop posting guides as literal text and actually process the user input entered into that field before trusting it, but the only defense against this attack until it was fixed was just to not click on any profiles, which was very disruptive.

WHAT DOES THIS TEACH US

1. **Switching services is not a defense** – as we can see, the kind of schemes attackers pull is the same across platforms: XSS, SQL injection, phishing, etc. Only using GOG or EA Origin isn't going to protect your games or your money.

2. **If you own a smartphone, use the Steam Guard Mobile Authenticator** – if you care about the security of your Steam account, there is not an excuse at this point.

3. **Be careful who you give permissions** – make sure that the site you're linking with your Steam account is really Discord or TeamSpeak or the TF2 Trading Outpost, etc.

4. **Don't download software outside of the Steam client** –the only Steam-related software you ever need to download besides the Steam client itself is the mobile app. The rest is malware.

5. As Gabe Newell said, **"Watch your credit card activity and statements closely."**

CONCLUSION

Using clients like Steam are unavoidable, and attackers will continue to be smarter than the average user. In spite of this, as long as Valve doesn't mess up to acutely with new features and continues to have reasonable patch times in regards to faults like the XSS vulnerability earlier this year, if you stay alert, you should be able to avoid becoming a victim.

Sources Cited

1. "Monthly Summaries -." SteamSpy - All the data about Steam games. https://steamspy.com/year/
2. Soper, Taylor. "Valve Reveals Steam's Monthly Active User Count and Game Sales by Region." GeekWire, 3 Aug. 2017, www.geekwire.com/2017/valve-reveals-steams-monthly-active-user-count-game-sales-region/.
3. "Valve's security philosophy" http://www.valvesoftware.com/security/
4. Deleon, Nicholas. "Valve's Steam Guard: Protecting Your Account From Evildoers Since 2011." (blog). http://social.techcrunch.com/2011/03/04/valves-steam-guard-protecting-your-account-from-evildoers-since-2011/
5. "Steam Guard - Account Recovery - Knowledge Base - Steam Support." https://support.steampowered.com/kb_article.php?ref=4020-ALZM-5519
6. "Valve's Online Game Service Steam Hit by Hackers - BBC News." http://www.bbc.com/news/technology-15690187
7. "Valve's Gabe Newell Offers Update on Steam Security Breach." *VentureBeat* (blog), February 10, 2012. https://venturebeat.com/2012/02/10/valve-update-on-steam-security-breach/
8. Peckham, Matt. "Steam Hack Worse than Thought…Three Months Later." *Time*. http://techland.time.com/2012/02/13/steam-hack-worse-than-thought-three-months-later/
9. "Phishy Steam Guard File Steals SSFN." Malwarebytes Labs, June 25, 2014. https://blog.malwarebytes.com/cybercrime/2014/06/phishy-steam-guard-file-steals-ssfn/
10. Elm Hoe. *Steam | How Accounts Are Getting Hacked. (FIXED)*. https://www.youtube.com/watch?time_continue=132&v=QPl_BJoBaVA&ab_channel=ElmHoe
11. "Regarding Gifting • r/DotA2." reddit. Accessed December 9, 2017. https://www.reddit.com/r/DotA2/comments/34kx7c/regarding_gifting/
12. "Steam News - Security and Trading." http://store.steampowered.com/news/19618/
13. "Malware Targeting Steam Traders Banks on New Escrow System." Malwarebytes Labs, December 9, 2015. https://blog.malwarebytes.com/cybercrime/2015/12/malware-targeting-steam-traders-banks-on-new-escrow-system/
14. "Steam News - Update on Christmas Issues." http://store.steampowered.com/news/19852/
15. "Steam News - Security and Trading: Update." http://store.steampowered.com/news/20631/
16. Lab, Kaspersky. "Steam on the Firing Line: How Cybercriminals Steal Gamers' Steam Accounts." https://www.kaspersky.com/blog/stealing-steam-accounts/11560/

17. "The Steam Community Exploit, Explained in-Depth by a Web Developer and /r/Steam Mod. • r/Steam." reddit. Accessed December 9, 2017. https://www.reddit.com/r/Steam/comments/5srlwd/the_steam_community_exploit_explained_indepth_by/
18. Goodin, Dan. "As Valve Eradicates Serious Bug in Steam, Here's What You Need to Know." Ars Technica, February 7, 2017. https://arstechnica.com/information-technology/2017/02/as-valve-eradicates-serious-bug-in-steam-heres-what-you-need-to-know/

Additional Sources

1. Grayson, Nathan. "Steam Users Think Valve's New Trading Restrictions Go Too Far." Steamed. https://steamed.kotaku.com/steam-users-think-valves-new-trading-restrictions-go-to-1762428792
2. May 02, Tom Sykes, and 2015. "Valve Explains the Reasoning behind Steam Gift Restrictions." pcgamer. http://www.pcgamer.com/valve-explains-the-reasoning-behind-steam-gift-restrictions/
3. O'Connor, Alice. "Warning Whistle: Beware a Possible Steam Security Hole." *Rock, Paper, Shotgun* (blog), February 7, 2017. https://www.rockpapershotgun.com/2017/02/07/steam-possible-security-hole/
4. "Phishers Bypass Steam Guard Protection." Malwarebytes Labs, April 17, 2014. https://blog.malwarebytes.com/cybercrime/2014/04/phishers-bypass-steam-guard-protection/
5. "Quote: Steam Hacked." *Time*. http://techland.time.com/2011/11/10/quote-steam-hacked/
6. "Trading and Market Restrictions - Trading and Gifting - Knowledge Base - Steam Support." https://support.steampowered.com/kb_article.php?ref=1047-edfm-2932
7. "Valve: DDoS Cyberattack Caused the Steam Caching Catastrophe (Cachetastrophe?)." *VentureBeat* (blog), December 30, 2015. https://venturebeat.com/2015/12/30/valve-ddos-cyberattack-caused-the-steam-caching-catastrophe-cachetastrophe/
8. "Valve Patches Trivial XSS Bug in Steam." Threatpost | The first stop for security news. https://threatpost.com/valve-patches-trivial-xss-bug-in-steam/123647/
9. "Valve Steam Service Experiences Security Breach." *VentureBeat* (blog), November 10, 2011. https://venturebeat.com/2011/11/10/valve-steam-service-experiences-security-breach/
10. Bailey, Matthew. "The Bug on the Forget Password Page Has Been Fixed. You Should Be Fine to Change Your Password Now If Required." Tweet. *@Cyborgmatt* (blog), July 5, 2015. https://twitter.com/Cyborgmatt/status/625095332100096004
11. Caldwell, Brendan. "Valve Restrict Steam Trading Again To Combat Cheaters." *Rock, Paper, Shotgun* (blog), August 5, 2016. https://www.rockpapershotgun.com/2016/08/05/valve-restrict-steam-trading-again-to-combat-cheaters/