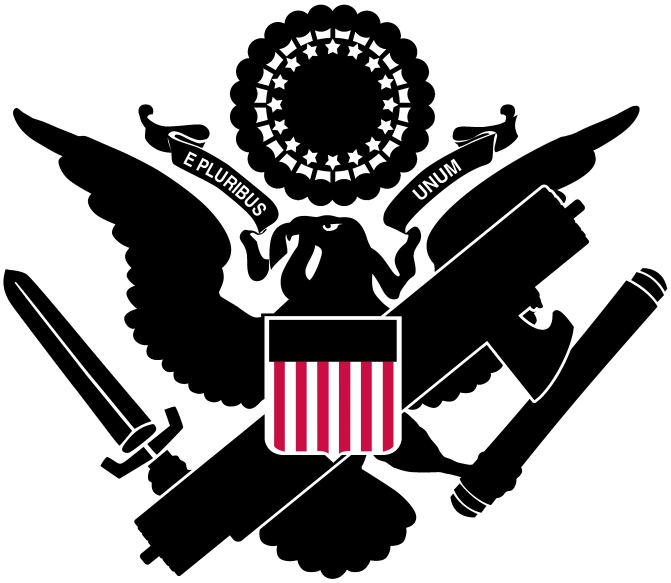
THE DISCORD SITUATION



NATIONAL FEDERALIST PARTY

SUBVERT.PW

BACKGROUND:

Discord, due to its ease of access and well designed interface quickly became the chat platform of choice for many people within the right wing in late 2015. It is believed that use of the application started on image boards where the application had gained traction through gaming. The easy link sharing invite system used by the application led to easy and quick adoption. However, in late 2016 discord came under (light) fire for believed data-mining. This led into further outcry after Discord shut down and banned users of right wing chat rooms after Charlottesville. This report is designed to investigate claims about the platform as well as look into alternatives for use.

DATA-MINING:

It is highly likely that discord is data-mining to generate revenue for the service, although this is unconfirmed. The first, direct indicator for this can be found within discord's source code. Within the javascript found on the web version of the client, Google API keys for geo-location have been found in plaintext. Locating users geographically is an important part of data-mining, and is needed to separate users by region.

The next big indicator of data-mining practices can be found within the discord TOS. In older versions of the document, Discord made statements that the company could transfer data to third "related" parties. The TOS has since been updated without such a statement. It is unknown if this update was made due to previous accusations of data mining or was simply due to changing needs.

It is also worth noting that the main founder of Discord, Jason Citron,was caught up in a data-mining scandal with a previous company known as OpenFeint. It is unknown if it was Citron's initial intent to make money through data mining, however if it was, this would create a clear pattern of creating social networks for gamers to gather and sell data.

While it is highly likely that data-mining is Discord's primary revenue source, all evidence leading to this conclusion is circumstantial. More information is needed before a definitive yes or no can be made. A possible route to proving this definitively could lie in its previous investors. Discord cannot sell the data on its own, and needs a third party with existing customers to purchase the data. Outright sale of information as Discord (or Hammer and Chisel, Discord's parent company) would be detrimental to their image.

SECURITY ISSUES:

Discord's improper implementation has led to serious problems in the past, turning small vulnerabilities into large exploits allowing attackers control of victim's computers. These problems primarily stem from the application's use of Electron.js. Electron is a framework used to turn node.js programs and html interfaces into full applications that can

be deployed cross platform. This is done through a pairing of the blink engine (from chrome) and a node.js interpreter. A slight problem arises from this. Javacript from outside sources displayed within electron is executed as node.js code unless displayed through a webview tag.

In no place within Discord is webview used to pad areas where user input is displayed. Should an xss vulnerability be found within the application, user machines can be exploited at the system level, rather than in the sandboxed environment of the web browser. Xss vulnerabilities have been found and patched in the application (most notably one involving the data: uri). It appears that Discord is aware of this problem, and has created a bug bounty system in an attempt to catch new flaws and minimize damage. However this will only do them so much good. Others have discovered discord's flaws, and sales of xss vulnerabilities may have occurred in secret (damagelab).

BAD BUSINESS PRACTICE:

While it has not been well documented, Discord has been using ethically questionable marketing tactics to bring discord to the public's eye. The core marketing strategy has always been paid promotion from youtube personalities, mainly in the gaming sector. In an attempt to build a userbase, the company paid youtubers to make discord channels and instructed them on how exactly to talk about the application.

Later, the company started a "hypesquad" system, giving kickbacks to users who promoted the product to friends. Members of hypesquad are encouraged to coordinate events, and receive boxes of Discord branded items to distribute. In return, those who advertise discord get a special member status. This advertising strategy is very lucrative, using people to advertise by word of mouth at little to no risk or cost.

CURRENT SITUATION:

DISCORD:

Discord views the right wing as a detriment to their platform, bringing them bad press coverage, and possibly scaring away investors. It has shown a willingness to ban and delete servers with right wing discussion. Its discovery of these servers appears to be done exclusively through user submitted reports as well as communication from anti-right wing groups. When banning a server, the platform tends to delete the server and suspend the accounts of the moderators and admins, leaving all others alone. It is not believed that discord looks through the personal chatlogs of the users it bans, or their chatlogs on other servers. Through the beginning of the ban spree, many moderators of servers were banned leaving other servers they started still open but without an owner.

UNICORN RIOT:

After the events of Charlottesville in 2017, Unicorn Riot published an expose on their website showing logs from a planning server. After this, Unicorn Riot began to publish numerous other leaks relating to Discord.

Unicorn Riot obtains its information primarily through infiltration. To log the chats in mass, the group uses the Discord History Tracker tool distributed by Daniel Chylek. It is not believed that Daniel works with Unicorn Riot or even has knowledge of their use of his tool. Unicorn Riot seems to have limited technical abilities. Their website is hosted via a paid wordpress instance. The discordleaks site is custom built on a rocket framework, implying the work of an ameture.

The group also currently faces problems with information overload. In one statement the group stated that they had 50-60 Discord servers to examine. The logs can reach anywhere from tens of thousands to hundreds of thousands of messages. With little technical skill to speed up the process and limited staff, analysis of this data has screeched to a halt. Analysis of Discord chat logs has become a resource sink for the group.

SPLC:

The SPLC has obtained information from right wing Discord chats in the past, and is working with Discord to help eliminate people from the platform. This is the beginning and the end of all knowledge regarding cooperation between these two groups. Speculation has long been made that Discord is giving chat logs to the SPLC, although there is no evidence at this time to confirm such an exchange.

ALTERNATIVES:

MATRIX/RIOT:

The biggest runner up against Discord is Matrix, an open chat standard similar to xmpp. Matrix's main chat client is Riot. Riot's current feature set can easily emulate the same functionality as Discord, and even offers end to end encryption with fingerprinting. Matrix's server system is federated, making the elimination of rooms and the banning of users much more difficult assuming users pick servers at absolute random while signing up and joining. There is one major security risk involved with Matrix. Theoretically speaking, a user could create a Matrix server specifically to honeypot right wing users, and log messages sent to the server. While no attack like this has been done, and checking to see if the attack is being executed is fairly simple, this is a risk that must be taken into account. Matrix servers that advertise themselves ad explicitly right wing should be regarded with some caution.

TELEGRAM:

The second runner up against discord is Telegram. Telegram is fairly secure, but has come under fire for "brewing its own crypto." Unlike Matrix, Telegram is centralized and requires a phone number before signing up. This is to limit users to a single account, and individualize their activities. For this reason, Telegram cannot be recommended.

WIRE:

Wire is another contestant in this. Wire is a direct competitor to Telegram, and has similar functionality. With end to end encryption and fingerprinting, the application is very secure. Its source code is also open to the public. Unlike telegram, it does not require a phone number, and is often considered better because of this. However, this application cannot bind multiple rooms together into one community like matrix or discord can, and users may find the transition hard. Business versions of the application display this feature, but require payment.