Background
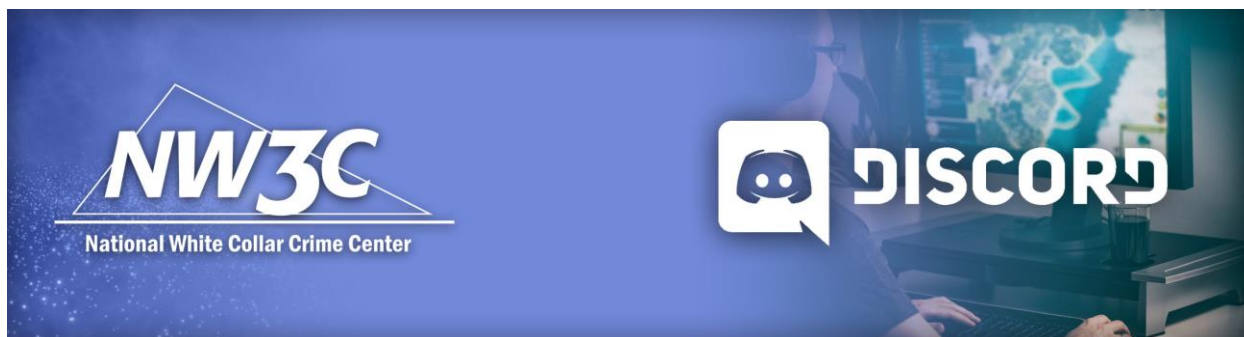
Discord was launched in May 2015 by Hammer & Chisel as a free, proprietary Voice over IP application, specifically marketed towards the "gaming" community.[1] The service features a lightweight desktop application as well as a mobile app, and a user will typically use the same account across both platforms. By December 2016, Discord had 25 million unique users and was processing over 120 million messages every month. [2]

What is Discord?

Discord provides free hosting for registered users to set up, configure, and customize their own communication servers, as well as a sleek and intuitive user interface for low-latency voice calls or persistent, IRC-like text chat rooms. Discord aims to provide an all-in-one experience, borrowing and improving upon many of the most popular features of similar services such as Skype and TeamSpeak, as well as adding unique features of its own, described below in the Interface and Features sections.

Discord can be accessed via web browser, at discord.gg, or by installing an application for a Windows, iOS, or Android device. New users register for the service with an email address, username, and password; after registering users have access to all of Discord's features.

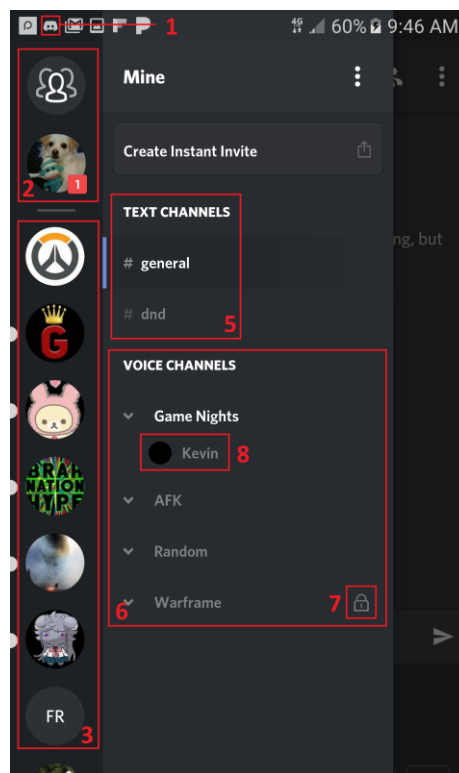Figure 1 is a screenshot of Discord version 3.3.3 running on a Samsung Galaxy S6 smartphone

Figure 1

1: This icon in the notifications bar indicates that the Discord application is in use.

2: The top icon acts as a shortcut to view an index of all private messages, sorted into a chronological order by sender, in a conversation-like format. The icon directly below shows that a private message is currently pending and is unread. The sender's profile icon is displayed along with the number of unread messages.

3: This tray shows all active servers that the user is a member of.

4: This bar shows the currently logged-in account on the device. Tap the text to show an overview of the account's profile.

5: This is a list of text-based channels in the currently selected server. Messages sent in these channels are persistent, stay visible, and are stored indefinitely. Uses can view and communicate in only one channel at a time, but can easily navigate among several by tapping the name of each channel.

6: This is a list of the voice channels on the currently selected server. Users can speak to and hear each other only when they are in the same voice channel. Voice channel navigation is the same as text-based channel navigation: by tapping the name of each channel. These can be navigated in the same manner as text channels, simply by tapping on the name of the channel.

7: This icon indicates that the selected voice channel is currently locked and inaccessible by your account.

8: This is a user in the voice channel "Game Nights." You can view this user's profile and a history of your conversations with him or her by tapping on the name and selecting "View Profile" from the drop down menu.

The User Account:

Users choose an alphanumeric username, which is then combined with a pound symbol (#) as well as a string of 4 or 5 randomized numbers, producing a unique "tag." This tag (example: NW3C_Test#3814) cannot be changed. The tag is publicly visible on an account's profile, and can be used for a variety of networking purposes inside of Discord, such as friend lists, server whitelists, and blocking other users.

Users can link other social media and entertainment services to their Discord account, and can automatically integrate features of those applications into their Discord usage. While information found on each of these social services is dependent on that user's privacy settings, all Discord profiles are public. As of January 2017, users can connect their Discord account to Steam, Twitch.TV, Reddit, Twitter, and Google+ accounts. Linked accounts can potentially provide investigative leads to law enforcement, as identifying account information can be found on each user's public Discord profile.

Importance to Law Enforcement

Discord's explosive growth shows no indication of slowing down. The large number of users paired with the gamer demographic creates a prime target for hackers. [3] Security experts at Symantec report that Discord is a huge distribution platform for hackers to obtain large amounts of traffic and malware executions. [4]

Investigative Information

Information Obtained via DiscordApp.com[5]

Discord is located at 401 California Drive, Burlingame, CA 94010. Legal process can be served through email at support@discordapp.com. Discord will divulge user information only if proper legal documents (subpoena, court order, search warrant are presented. Requests must include the following:

- The user's full (non-unique name + identifying string) Discord tag
- The specific information that is requested and its pertinence to the investigation

The privacy policy states that Discord stores identifying information (like the email address used to register an account and a history of IP addresses), and usage information (such as chat logs, login sessions, and device information). Discord also collects information from any third-party application linked to a user's profile, as well as advertising profiles on certain users. [6]

Information Retrieved from an iOS Device

The National White Collar Crime Center (NW3C) Cybercrime Section downloaded, installed, and used the Discord application version 3.3.3 on an Apple iPod Touch, 5th Generation model A1509 running iOS version 9.3.5. The test machine was an Apple MacBook Pro running MacOS Sierra. A logical extraction of the device was completed using BlackBag Technologies Blacklight 2016 Release 3. A manual search of the results and keyword search for the word "Discord" located several potentially useful artifacts during the examination. The files and folders of interest were exported then viewed manually with database and property list viewers. In order to replicate, it is recommended to image the device before opening the app as using the app can change some of these values.

All time values are recorded in Unix time. This counts the number of seconds that have passed since January 1st, 1970. Convert the numbers listed here to readable dates using www.epochconverter.com

- com.hammerandchisel.discord.plist, with the path of /Root/mobile/applications/com.hammerandchisel.discord/Library/Preferences, has one value of interest.

- o iRateFirstUsed – this value appears to be the time and date the application was first used on the device. This value does not reset if the application is uninstalled and reinstalled at a later time.
- Manifest.json, with the path of /Root/mobile/applications/com.hammerandchisel.discord/Documents/RCTAsyncLocalStorage_V1, has one value of interest.
  - o lastConnectedTime – this value appears to be the most recent online usage of the application.
- com-facebook-sdk-AppEventsTimeSpent.json, with the path of /Root/mobile/Applications/com.hammerandchisel.discord/Library, has two values of interest.
  - o secondsSpentInCurrentSession – this value indicates how long the application was open and being used in its most recent instance.
  - o lastSuspentTime – this value indicates the last time the application was manually, forcibly closed to prevent it from running in the background.

Information Retrieved from an Android Device

The National White Collar Crime Center (NW3C) Cybercrime Section downloaded, installed, and used the Discord application version 3.3.3 on a Samsung Galaxy S4 model SCH-R970. The test machine was a Dell Latitude E6500 running Windows 8.1 Enterprise. A logical extraction of the device was completed using MSAB's XRY. A manual search of the results and keyword search for the word "Discord" located several potentially useful artifacts during the examination. The files and folders of interest were exported then viewed manually with another MSAB product, XAMN. In order to replicate, it is recommended to image the device before opening the app as using the app can change some of these values.

All time values are recorded in Unix time. This counts the number of seconds that have passed since January 1st, 1970. Convert the numbers listed here to readable dates using www.epochconverter.com.

- com.discord_preferences.xml, with the path of /userdata/data/com.discord/shared_prefs, has one value of interest.
  - o PREFS_LAST_KNOWN_EMAIL – this value contains a string with identifying information, the email address of the account most recently used on the device.
- com.google.android.gms.measurement.prefs.xml, with a path of /userdata/data/com.discord/shared_prefs, has two values of interest.

- o last_stop_time – this value indicates this value indicates the last time the application was manually, forcibly closed to prevent it from running in the background.
  - o last_upload – this value appears to be the most recent online usage of the application.
- Cached thumbnails of every image sent through the application can be found at the following path: /userdata/media/0/Pictures/Discord
- Cached thumbnail covers of every image received through the application can be found in folders unique to each conversation with each user or shared server. This type of file hierarchy, while containing no identifying information on the users who sent the images, allows an investigator to categorize each image by its source. If the source of one of the images can be identified, every other image in that folder can be tied to that same source. These folders can be found at the following path: /userdata/data/com.discord/cache/app_images_cache_small/

Feedback

For additional information or suggestions please contact cyberalerts@nw3c.org

Sources

1 https://discordapp.com/features
2 Kerr, Chris. "Booming game chat app Discord intros in-game text, voice integration." Gamasutra. 8 Dec. 2016. Web.
3 "Data Privacy and Online Gaming: Why Gamers Make for Ideal Targets." TrendMicro. 25 Oct. 2016. Web.
4 Beltov, Martin. "Hackers Use the Discord App to Deliver Malware." Best Security Search. 27 Feb. 2017. Web.
5 https://discordapp.com/company
6 https://discordapp.com/privacy