

Grand Theft Auto VI Hype Leads to Malware

 huntress.com/blog/fake-gta6-download-malware-analysis

Matt Poto, Ben Nahorney



Acknowledgments: Special thanks to Jon Semon, Andrew Brant, and Lindsey O'Donnell-Welch for their contributions to this investigation and writeup.

Background

There's still three months until the release of Grand Theft Auto VI (GTA6), but the internet has already reached a fever pitch thanks to a slate of [gameplay footage leaks](#), as well as an [official extended look](#).

Not to let such a hot topic pass them by, threat actors are capitalizing on the GTA6 popularity to distribute malware, compromising overly eager fans hoping to get their hands on early release versions of the game. However, there is no official GTA6 demo as of yet, nor is there currently any sign of an actual leaked, playable copy of the game being distributed online.

Bad actors have instead been busy distributing malware masquerading as optical disk image files (ISOs) of the game. While there have been [several writeups on these threats](#), we found a sample in a sandbox with different functionality.

A variety of distribution methods

Malicious actors appear to be covering a variety of avenues where an overeager fan may attempt to find a copy of the game. We have seen several examples of [SEO poisoning](#) designed to rank highly in searches for GTA6, as well as ISOs published on [gaming forums](#) and various torrenting sites. There have also been social media posts advertising these ISOs.

Some of the ISOs being distributed can be very large in size—some crossing 100GB. However, this appears to be done simply to emulate the size an ISO might be for a AAA video game, and the file itself is filled with junk data to reach a plausible size. The malicious files contained within are a factor smaller.

What one ISO can do

The sample that we obtained contained several components. The malicious actors behind it appear to be making an opportunistic attempt at compromising systems, throwing everything they can at the users who attempt an installation. The ISO includes a fake installer, several RATs, an infostealer, ransomware being used as a wiper, and a web browser.

When a target mounts and opens the ISO for the supposed game, they're presented with the main installer file, `gta6installer.exe`, which curiously has a GTA5 logo for its icon.



Figure 1: Icon for the main installer file

Executing this file starts an installer that displays a message in Russian:

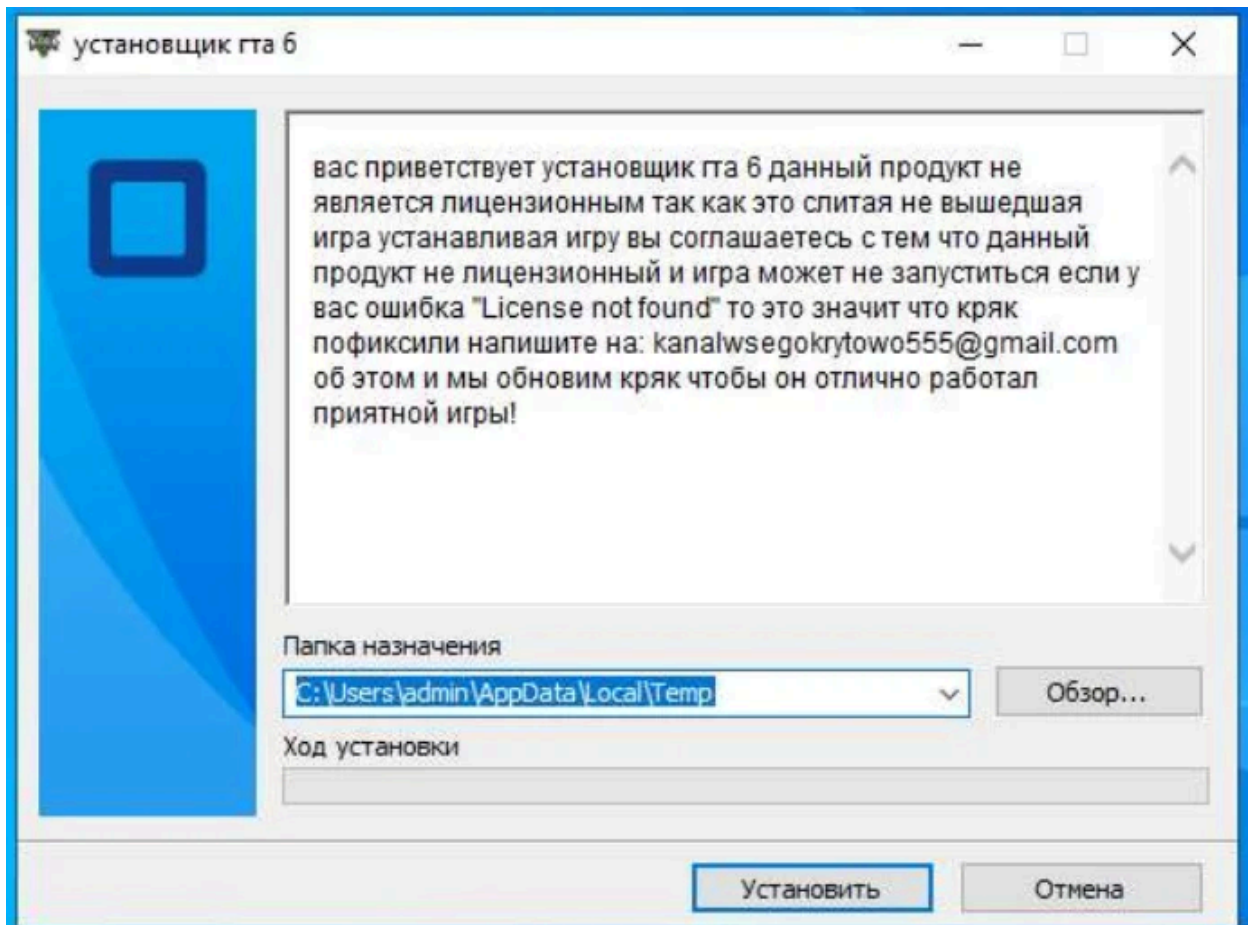


Figure 2: Message contained within the fake GTA6 installer

Using online tools, this message roughly translates to the following in English:

Welcome to the GTA 6 installer. This product is not licensed because it is a leaked, unreleased game. By installing the game, you agree that this product is unlicensed and that the game may not start. If you receive the error "License not found," it means that the crack has been fixed. Write to kanalwsegokrytowo555@gmail.com about it, and we will update the crack so that it works perfectly. Enjoy the game!

The setup here is that the threat actor is warning the user that this installer may not work and to watch for a "License not found" error. They provide an email to contact them to update the supposed crack that would make this game work (when this installation is complete, a message with exactly this text is deliberately displayed).

We attempted to contact the email address provided, but as of publication we have not received a response to our inquiry.

The malware contained within the ISO appears to be fairly old, repurposed for this opportunistic attack, with files dating back to 2023 in many cases. Proceeding with the installation, several files are added to the %TEMP% folder on the system, many of which appear to be GTA6-branded to avoid suspicion.

- %TEMP%\checkinternetconnection.bat

- %TEMP%\find.vbs
- %TEMP%\licensechecker.exe
- %TEMP%\rockstar.exe
- %TEMP%\steam.exe
- %TEMP%\rockstargames.exe
- %TEMP%\gta6.exe
- %TEMP%\YandexPackLoader.exe
- %TEMP%\license.exe
- %TEMP%\rockstargamescrashfixer.exe
- %TEMP%\rockstarservices.exe
- %TEMP%\adminapp.exe

The checkinternetconnection.bat file then launches Microsoft Edge and connects to [https://clck\[.\]ru/34uJnp](https://clck[.]ru/34uJnp), where it confirms that it has an internet connection before proceeding to unpack and install the various malware components.

NJRAT

There are several copies of NJRAT installed on the system:

- licensechecker.exe launches %TEMP%\any.ran.exe
- rockstar.exe launches %TEMP%\svchost.exe
- steam.exe launches %TEMP%\abc.exe

This is a pretty well-known RAT that includes a variety of features, such as:

- Opening a shell
- Logging keystrokes
- Accessing connected cameras
- Stealing credentials from browsers
- Uploading and downloading files
- Modifying files, registry entries, and processes
- Viewing the desktop and taking screenshots

- Stealing cryptocurrency details

Each of these NJRAT instances create Windows Firewall rules for themselves and then they connect to several IP addresses associated with AWS-hosted infrastructure:

- 35.157.111[.]131
- 3.68.56[.]232
- 3.67.15[.]169

They also connect to secure tunneling services provided by ngrok at 7.tcp.eu.ngrok[.]io:12684.

Three more copies of NJRAT (`license.exe`, `rockstargamescrashfixer.exe`, and `rockstarservices.exe`) were installed to %TEMP%, but didn't spawn any children, make any network connections, or exhibit any further, observed activity. Clearly this was a case of a threat actor throwing an armful of RATs at the wall and seeing what would stick.

DCRAT

The `rockstargames.exe` file drops a `.bat` file in %TEMP%\P3usMXh1h4.bat, which sets the ntp server to local, installs a randomly named copy of DCRAT in the C:\Users\Default\Local Settings\ folder, in our case as `User00BEBroker.exe`, and then deletes itself.

The RAT then connects to `a0700877.xsph[.]ru` (141.8.197[.]42). This domain has been on blocklists for several years, categorized as known malicious infrastructure. This instance of DCRAT allows for general control of the compromised system, including the following capabilities:

- Capturing screenshots
- Mouse control
- Audio device discovery
- Window tracking
- Clipboard access
- Read/write access to the registry

The `rockstargames.exe` file then modifies the Windows hosts file in order to sinkhole various telemetry and residential antivirus reporting services.

```

# Start of entries inserted by Spybot Anti-Beacon for Windows 10 Optional
# End of entries inserted by Spybot Anti-Beacon for Windows 10 Optional
# Start of entries inserted by Spybot Anti-Beacon for Windows 10
# This list is Copyright 2000-2017 Safer-Networking Ltd.
0.0.0.0 app.adjust.com
0.0.0.0 app.adjust.io
0.0.0.0 app-sj01.marketo.com
0.0.0.0 t.appsflyer.com
0.0.0.0 analytics.ff.avast.com
0.0.0.0 analytics.ns1.ff.avast.com
0.0.0.0 v7event.stats.avcdn.net
0.0.0.0 v7.stats.avcdn.net
0.0.0.0 ads.avocet.io
0.0.0.0 telemetry.battle.net
0.0.0.0 analytics.rollout.io
0.0.0.0 metrics.ol.epicgames.com
0.0.0.0 a.fiksu.com
0.0.0.0 sdk.fiksu.com
0.0.0.0 settings.crashlytics.com
0.0.0.0 e.crashlytics.com
0.0.0.0 insights-collector.gog.com
0.0.0.0 ssl.google-analytics.com
0.0.0.0 ssl-google-analytics.l.google.com
0.0.0.0 static.hotjar.com
0.0.0.0 flow.lavasoft.com
0.0.0.0 telemetry.servers.getgo.com
0.0.0.0 telemetry.malwarebytes.com
0.0.0.0 ws.mcafee.com
0.0.0.0 analytics.ccs.mcafee.com
0.0.0.0 analyticsdcs.ccs.mcafee.com
0.0.0.0 gate.hockeyapp.net
0.0.0.0 api.mixpanel.com
0.0.0.0 decide.mixpanel.com
0.0.0.0 ads.mopub.com
0.0.0.0 incoming.telemetry.mozilla.org
0.0.0.0 h.online-metrix.net
0.0.0.0 analytics.paddle.com
0.0.0.0 treasuredata.com
0.0.0.0 in.treasuredata.com
0.0.0.0 redshell.io
0.0.0.0 api.redshell.io
0.0.0.0 carcharodon.trendmicro.com
0.0.0.0 cdn.segment.com
0.0.0.0 api.segment.io
0.0.0.0 mobile-service.segment.com
# End of entries inserted by Spybot Anti-Beacon for Windows 10

```

I

Figure 3: Entries added to the hosts file

Mercurial Grabber

The Mercurial Grabber infostealer is dropped alongside the other files from the ISO install as `adminapp.exe`. This is an infostealer that is readily available on GitHub, and while it is advertised as being for "educational purposes only," it's clearly not being used in such a manner here. The infostealer allows for the collection of the following information:

- Roblox Studio cookies
- Minecraft session data

- Discord tokens
- Google Chrome passwords and cookies
- System information, IP address, and geolocation
- Windows product keys
- Screenshots

The infostealer then uses Discord webhooks to send the information it steals to the following URL:

`https://discord[.]com/api/webhooks/995445114254139543/NmpxQmuBCD6sm3UkVvupGtx-Y0M_A86oJHp000-l8F4jakfVhqFXzMBoy1uBDdj2rBLc`

Chaos ransomware

While this is technically a well-known ransomware family, it appears that the actors are not looking to collect a ransom from infected users. Instead, they encrypt and/or destroy files on the system, effectively utilizing the ransomware as a wiper.

This instance of the ransomware will only run if the user is an administrator. First, the `gta6.exe` file creates `%USERPROFILE%\AppData\Roaming\svchost.exe`. The ransomware then disables recovery options, deleting all backup shadow copies of the drives and modifying the boot configuration to disable recovery and ignore any boot failures. It then changes the desktop wallpaper to an image of SpongeBob with a message in Russian:

YOU HAVE BEEN HACKED BY THE ASHA HACKER TEAM!

ВЫ ВЗЛОМАНЫ ХАКЕРСКОЙ КОМАНДОЙ АША!

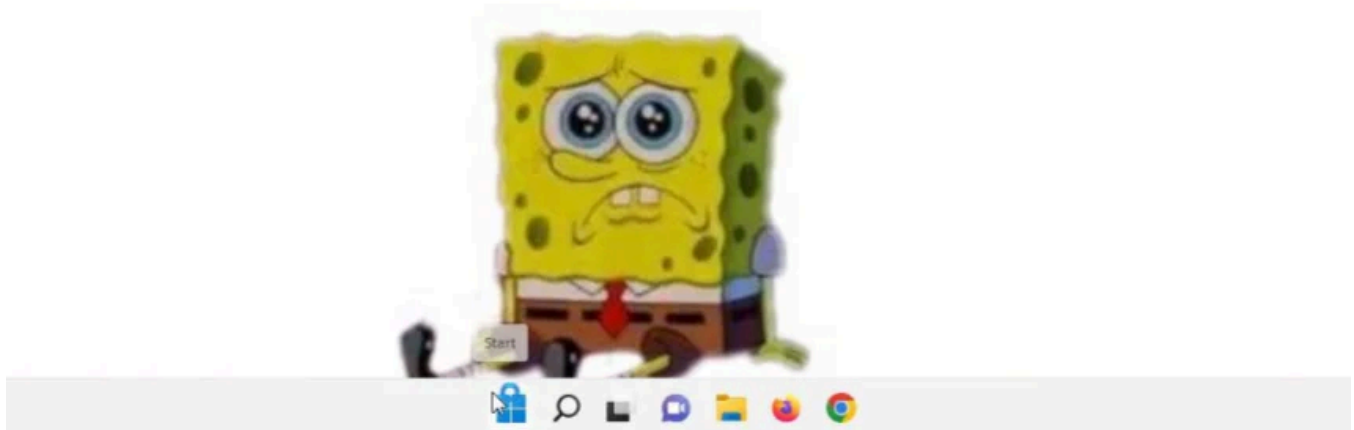


Figure 4: Changes to the desktop wallpaper

The ransomware encrypts files 200MB and smaller, by first creating a random password of 20 characters, then using it to run AES encryption, and finally adding a random four-character extension to the files. Any files larger than 200MB are overwritten with random data, effectively destroying them. It encrypts any non-system drives first, before running through the following user and shared-data locations on the system drive, as well as OneDrive drives, if present:

- %USERPROFILE%\Desktop
- %USERPROFILE%\Links
- %USERPROFILE%\Contacts
- %USERPROFILE%\Documents
- %USERPROFILE%\Downloads
- %USERPROFILE%\Pictures
- %USERPROFILE%\Music
- %USERPROFILE%\Saved Games

- %USERPROFILE%\Favorites
- %USERPROFILE%\Searches
- %USERPROFILE%\Videos
- %APPDATA%
- %ONEDRIVE%

Finally, it creates a ransom note text file in each folder named `read_it.txt`.



Figure 5: Ransomware note

```
hello, your files has been encrypted by achvzlom
i don't have paypal or other banks so you don't can donate me :XD
so, your files has been encrypted forever
achvzlom company
ach ransomware
```

Unfortunately for anyone seeing this message, it does not appear that the threat actors are looking to collect a ransom, effectively turning this malware into a wiper, as opposed to a standard ransomware attack.

A browser, just for kicks

Finally, the ISO installs a copy of the Yandex Browser, as `YandexPackLoader.exe`. The reasons for installing this browser remain unclear; however, this is a popular browser in eastern Europe and Russia.

Given the installer's use of Russian and the presence of this browser, it's possible that this ISO was initially designed to target users in this region.

A plausible failure

As the installation completes, the threat launches `WScript.exe` and loads `find.vbs`, which displays a message that says "license not found" on the screen.

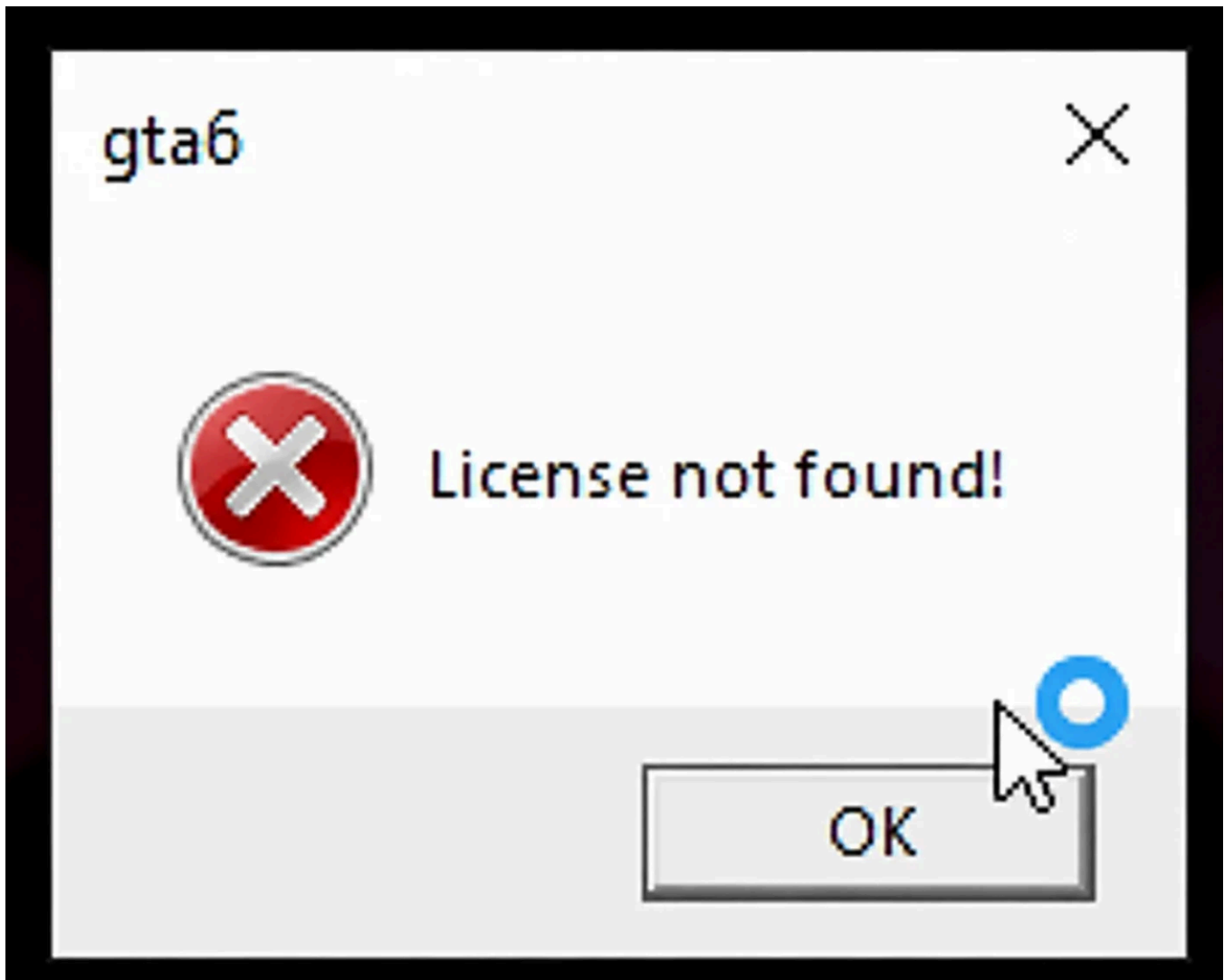


Figure 6: Error message meant to trick the user into thinking the game didn't install

This message is exactly what the installation warned about, leaving the user with a plausible explanation for why no game ran and diverting their attention from the malware being installed in the background.

Mitigation Guidance

Generally speaking, it's not a good idea to attempt to download cracked, pirated software, especially if the game in question has not yet been released. This is fertile ground for scams and threat actors attempting to take advantage of the impatient and overeager.

The good news here is that nothing in this ISO is all that new or relatively novel. The malware contained within is several years old, and for each case, a currently updated version of Windows Defender can detect the malware and stop it from compromising the system. However, if you do install this malware, the best practice is to disconnect the machine from the network, reset all of your passwords, enable 2FA wherever possible, and do a complete reimage of the compromised system.

Indicators of Compromise (IOCs)

Item	Description
Gta6installer.exe MD5: a15e280a3fd65dfaa243bbe2dbf45e97	Initial installation executable
%TEMP%\checkinternetconnection.bat MD5: 6b49f24d5d5b49127476bc385565f8b0	BAT file used to confirm a working internet connection

%TEMP%\licensechecker.exe	Copies of NJRAT and associated launchers
%TEMP%\rockstar.exe	
%TEMP%\steam.exe	
%TEMP%\any.ran.exe	
%TEMP%\svchost.exe	
%TEMP%\abc.exe	
%TEMP%\license.exe	
%TEMP%\rockstargamescrashfixer.exe	
%TEMP%\rockstarservices.exe	
MD5s:	
2a0834560ed3770fc33d7a42f8229722	
57b9c56ef97a7ada98257b23577bf5e3	
60a0f58001ea7be538cd42b651924cc7	
15eca4a3f7350423cf4db0b4c30d1968	
Ea991bc9334b36a6b958f564ee716776	
2a385fe7bed9899d77d05cb8e302d557	
35.157.111[.]131	IP and ngrok addresses that NJRAT connects to
3.68.56[.]232	
3.67.15[.]169	
3.68.56[.]232	
7.tcp.eu.ngrok[.]io:12684.	

%TEMP%\rockstargames.exe

%TEMP%\P3usMXh1h4.bat

C:\Users\Default\Local Settings\[RANDOM FILE NAME].exe

Copy of
DCRAT and
associated
installation
files

MD5:

8da3fe3664d81226b0fb2a50a0537d4f

0.0.0.0 app.adjust.com
0.0.0.0 app.adjust.io
0.0.0.0 app-sj01.marketo.com
0.0.0.0 t.appsflyer.com
0.0.0.0 analytics.ff.avast.com
0.0.0.0 analytics.ns1.ff.avast.com
0.0.0.0 v7event.stats.avcdn.net
0.0.0.0 v7.stats.avcdn.net
0.0.0.0 ads.avocet.io
0.0.0.0 telemetry.battle.net
0.0.0.0 analytics.rollout.io
0.0.0.0 metrics.ol.epicgames.com
0.0.0.0 a.fiksu.com
0.0.0.0 sdk.fiksu.com
0.0.0.0 settings.crashlytics.com
0.0.0.0 e.crashlytics.com
0.0.0.0 insights-collector.gog.com
0.0.0.0 ssl.google-analytics.com
0.0.0.0 ssl-google-analytics.l.google.com
0.0.0.0 static.hotjar.com
0.0.0.0 flow.lavasoft.com
0.0.0.0 telemetry.servers.getgo.com
0.0.0.0 telemetry.malwarebytes.com
0.0.0.0 ws.mcafee.com
0.0.0.0 analytics.ccs.mcafee.com
0.0.0.0 analyticsdcs.ccs.mcafee.com

Entries
added to the
host file by
DCRAT

0.0.0.0 gate.hockeyapp.net
0.0.0.0 api.mixpanel.com
0.0.0.0 decide.mixpanel.com
0.0.0.0 ads.mopub.com
0.0.0.0 incoming.telemetry.mozilla.org
0.0.0.0 h.online-metrix.net
0.0.0.0 analytics.paddle.com
0.0.0.0 treasuredata.com
0.0.0.0 in.treasuredata.com
0.0.0.0 redshell.io
0.0.0.0 api.redshell.io
0.0.0.0 carcharodon.trendmicro.com
0.0.0.0 cdn.segment.com
0.0.0.0 api.segment.io
0.0.0.0 mobile-service.segment.com

a0700877.xsph[.]ru
(141.8.197[.]42)

Domain and
IP address
that DCRAT
connects to

%TEMP%\adminapp.exe

MD5:

dfdf5e5b78d2ec764c0e5641cf9a0d26

Mercurial
Grabber
infostealer
binary

https://discord[.]com/api/webhooks/995445114254139543/NmpxQmuBCD6sm3UkVvupGtx-Y0M_A86oJHp000-l8F4jakfVhqFXzMBoy1uBDdj2rBLc	Discord webhook that Mercurial Grabber connects to
%TEMP%\gta6.exe	Chaos ransomware binaries
%USERPROFILE%\AppData\Roaming\svchost.exe	
MD5: b9648ec8cc806e7661aabcfc91dc836c	
read_it.txt	Ransomware note left in folders with Chaos ransomware-encrypted files
%TEMP%\YandexPackLoader.exe	Yandex web browser
MD5: 1ec9eff863dc4418d1498bc3d904899d	
%TEMP%\find.vbs	
MD5: 0e39e8d7b641bcda4376ebbfef7b12e	Script that displays a "license not found" message