

Forum:[Hack Forums](#)

Thread: [RAT for Mac osx](#)

creatine - November 7, 2019, 5:13 am

Looking to find Rat for mac must work latest editions, cheers

Mitch - November 14, 2019, 4:27 pm

Use a java-based rat. I can't name any for you but they're out there.

tysonnuggets666 - November 17, 2019, 1:12 am

(Nov 14, 2019 05:27 PM)Mitch Wrote: [\[CITE\]](#) Use a java-based rat. I can't name any for you but they're out there.

Yeah if they lookup "Java RAT Github" a ton of stuff comes up.

creatine - November 17, 2019, 8:21 am

(Nov 14, 2019 05:27 PM)Mitch Wrote: [\[CITE\]](#) Use a java-based rat. I can't name any for you but they're out there.

Many Thanx

(Nov 17, 2019 02:12 AM)tysonnuggets666 Wrote: [\[CITE\]](#) Yeah if they lookup "Java RAT Github" a ton of stuff comes up.

Thanks again super, but the target mac should have allready java instaled?

tysonnuggets666 - November 17, 2019, 9:53 am

(Nov 17, 2019 09:21 AM)creatine Wrote: [\[CITE\]](#) Many Thanx

Thanks again super, but the target mac should have allready java instaled?

I don't think so you could convert it over to a binary for your target platform and most machines run it anyways.

CyberStrike - November 19, 2019, 5:48 pm

Learn about OSX what protections are in place, what scripting languages are out of the box supported. You will quickly find that with a bit of bash or python scripting you can really end up getting access. Be very familiar with BASH and the nuances of OSX's castrated BASH.

Root-Senpai - November 19, 2019, 5:50 pm

There are many available in GitHub that you can practice and learn with. make sure to use on your own setup to understand how to use it properly and learn the ropes before practical use

<https://github.com/Marten4n6/EvilOSX>

here is an example, can not vouch for how good it is, probably some better projects out there, but it was the first that popped up in my memory lol

kayla_90 - November 19, 2019, 7:07 pm

look for EggShell in github

creatine - November 20, 2019, 12:36 am

(Nov 19, 2019 06:50 PM)Root-Senpai Wrote: [\[CITE\]](#) There are many available in GitHub that you can practice and learn with. make sure to use on your own setup to understand how to use it properly and learn the ropes before practical use

<https://github.com/Marten4n6/EvilOSX>

here is an example, can not vouch for how good it is, probably some better projects out there, but it was the first that popped up in my memory lol
i am testing this tomorrow get rubber ducky. ?

(Nov 19, 2019 08:07 PM)kayla_90 Wrote: [\[CITE\]](#) look for EggShell in github
i will check this out ? ordered the teensy usb dev board is here tomorrow, tonight ducky night. evil laughter

creatine - November 29, 2019, 1:57 am

When i put the rubberdukey (payload evil osx) in the usb slot, mac osx start asking to indentify the keyboard and telling me to press the right key next the left shift key?

But there is no button to press on the ducky because its not a keyboard offcourse. i started the server allready on kali port 4446, but no client pops up on the server.
???

creatine - December 2, 2019, 5:55 am

Solution found :

<https://null-byte.wonderhowto.com/how-to/hack-macos-with-digispark-ducky-script-payloads-0198555/>

Root-Senpai - December 2, 2019, 6:11 am

(Nov 29, 2019 02:57 AM)creatine Wrote: [\[CITE\]](#) When i put the rubberdukey (payload evil osx) in the usb slot, mac osx start asking to indentify the keyboard and telling me to press the right key next the left shift key?

But there is no button to press on the ducky because its not a keyboard offcourse. i started the server allready on kali port 4446, but no client pops up on the server.
???

test on the machine without rubberdukey first to make sure ur using it properly, also what payload u using?

and when it tells u to press key it is on the keyboard connected to the device, not the rubberdukey

(Dec 2, 2019 06:55 AM)creatine Wrote: [\[CITE\]](#) Solution found :

<https://null-byte.wonderhowto.com/how-to/hack-macos-with-digispark-ducky-script-payloads-0198555/>

sorry didnt see this post ! glad you found it :)

creatine - December 2, 2019, 6:22 am

can this thread be placed in the right section : Remote Administration Tools

SIM-4199941 - December 9, 2019, 7:08 am

(Nov 7, 2019 06:13 AM)creatine Wrote: [\[CITE\]](#) Looking to find Rat for mac must work latest editions,

cheers

iWorm Botnet for Mac =) ?

creatine - December 9, 2019, 11:17 pm

(Dec 9, 2019 08:08 AM)salegrosso Wrote: [\[CITE\]](#) iWorm Botnet for Mac =) ?

More info please, where to find? ?

SIM-4199941 - December 10, 2019, 7:06 am

(Dec 10, 2019 12:17 AM)creatine Wrote: [\[CITE\]](#) More info please, where to find? ?

[HERE](#)

creatine - December 11, 2019, 12:28 am

Technical Details

Backdoor:OSX/Iworm is reportedly spread via pirated software downloads. Once present on a machine running the Mac OS X operating system, the malware installs a file in the Library directory and then connects to Reddit's search page.

An unusual feature of this malware and the botnet it connects to is that a specific subreddit was used to distribute the IP addresses of the botnet's command and control (C&C) servers to affected machines. The subreddit has since been cleared of this C&C-related data, and the account used to post the data was shut down.

If the affected machine does successfully connect to the botnet, it is able to carry out a range of instructions, including downloading a file, executing a system instruction and changing its own configuration file. At the time of writing, there have been no reports of the IWorm botnet being used for malicious activities.

Following public reports of the malware, Apple updated OS X's built-in XProtect component to include identification for this malware.

Therefore dont work on Mojave, Catalina etc From 10.12 no more useable. But thanks anyway

Got my Digispark ATtiny85 Micro USB, gonna test tonight with evilosx, and program the digispark, so the mac thinks its a real apple keyboard.

general79 - December 15, 2019, 1:58 am

Need a good rat for Mac OS X , Android and Linux. Will pay for the service

nexis - December 15, 2019, 5:03 am

EvilOSX works decently well. I don't know on what criteria I can judge a RAT. However, recent version of macOS do not have the JVM pre installed. Do Java-based RATs require Java to be preinstalled on the machine?

Also, Null Byte has some good stuff on Macs.

<https://null-byte.wonderhowto.com/how-to/hacking-macos-create-undetectable-payload-0189715/>

It seems that TokyoNeon has a script called Armor (<https://github.com/tokyoneon/Armor>) which can evade AV... I presume that this will be very useful.

creatine - December 16, 2019, 4:52 am

(Dec 15, 2019 06:03 AM)nexis Wrote: [\[CITE\]](#) EvilOSX works decently well. I don't know on what criteria I can judge a RAT. However, recent version of macOS do not have the JVM pre installed. Do Java-based RATs require Java to be preinstalled on the machine?

no not needed.

Also, Null Byte has some good stuff on Macs.

<https://null-byte.wonderhowto.com/how-to/hacking-macos-create-undetectable-payload-0189715/>

It seems that TokyoNeon has a script called Armor (<https://github.com/tokyoneon/Armor>) which can evade AV... I presume that this will be very useful.

Yes this looks usefull, ?

nexis - December 16, 2019, 3:46 pm

(Dec 16, 2019 05:52 AM)creatine Wrote: [\[CITE\]](#) Yes this looks usefull, ?

Also man, I'm currently doing some stuff on this specific OS... Let's keep each other updated. I don't think there are many people on here interested/using Macs; it isn't that different from Linux tools, but at the same time, I think that there is most definitely an interesting thing to explore, since there are so few tools and so few people trying to exploit Macs.

(If there are a lot more people using macOS, please let me know!)

creatine - December 17, 2019, 3:48 am

Yes lets help each other to make a nice recent macosx Rat. hidden in doc or pdf, goes trough mail.