

Forum:[Hack Forums](#)

Thread: [PoC Reverse Engineering and Software Architecture Services](#)

7psy - June 23, 2021, 9:41 am

Hey all,

Is there anyone who can share their experiences with proof-of-concept reverse/malware engineering, Oday development and /or software architecture and implementation design services ? I heard of iYSRED that is a top-notch research laboratory providing lots of resources among the services/solutions provided on their page. Let's do some brainstorming here ! ?
[contract=tid]Start Contract[/contract]

x_x - June 23, 2021, 9:50 am

I made a POC iOS ransomware for jailbroken users, stops them from unlocking the device, locks all files, if they attempt to reboot then the /var/ gets deleted. No c2 as it was just POC so I didn't add a way to buy a decryption key.

7psy - June 23, 2021, 5:43 pm

(Jun 23, 2021 09:50 AM)Yatzz Wrote: [\[CITE\]](#) I made a POC iOS ransomware for jailbroken users, stops them from unlocking the device, locks all files, if they attempt to reboot then the /var/ gets deleted. No c2 as it was just POC so I didn't add a way to buy a decryption key.

Have you tried accessing local user hash table to further bruteforce for privilege escalation scenarios ?

x_x - June 23, 2021, 11:21 pm

(Jun 23, 2021 05:43 PM)7psy Wrote: [\[CITE\]](#) Have you tried accessing local user hash table to further bruteforce for privilege escalation scenarios ?

It already has root permissions as soon as it is executed due to "filza" (the file manager for jailbroken devices) installing every .deb (debian) as root which is kinda a huge oversight.

7psy - June 25, 2021, 12:24 pm

(Jun 23, 2021 11:21 PM)Yatzz Wrote: [\[CITE\]](#) It already has root permissions as soon as it is executed due to "filza" (the file manager for jailbroken devices) installing every .deb (debian) as root which is kinda a huge oversight.

Interesting. I thought cross compiling would be possible. On the other hand I was mentioning about a hypothetical device that was not jailbroken thus a local day might escalate to root access. From my perspective execution can occur if file manager is something else as well. Also there might be relation the emmc driver circuit and firmware too.

x_x - June 25, 2021, 12:33 pm

(Jun 25, 2021 12:24 PM)7psy Wrote: [\[CITE\]](#) Interesting. I thought cross compiling would be possible. On the other hand I was mentioning about a hypothetical device that was not jailbroken thus a local day might escalate to root access. From my perspective execution can occur if file manager is something else as well. Also there might be relation the emmc driver circuit and firmware too.

The post probable way is by iOS webkit, there is a public ios 9.3.3 webkit exploit to shell from a link

7psy - June 26, 2021, 9:01 am

(Jun 25, 2021 12:33 PM)Yatzz Wrote: [\[CITE\]](#) The post probable way is by iOS webkit, there is a public ios 9.3.3 webkit exploit to shell from a link

Dunno abbott the sploit but there sure exists a vector through the transport layer as well. If you don't have x permission over shell webkit makes no sense already. Why don't you focus on new architectures, I mean 9 is way too old and has no use at all. There are rumors floating around on various vehicle control and entertainment softwares, there is plenty of money in that bussines, if you know how to code C or Assembly ?