

Forum: [Hack Forums](#)

Thread: [Idea I had for exploiting machines.](#)

Mr. Robot - July 8, 2019, 3:49 am

I'm not quite sure how this would play out yet as I assume most paths are clearly patched.

Say a program like Chrome is installed and we can see that through a man in the middle attack (headers).

We see an update for the browser has been released or just about to be released that day.

What if we grab that certificate for the browser update and craft a malicious replacement for the man in the middle attack.

Same would apply for Windows or Adobe applications - surely there must be something that's vulnerable through that. I haven't personally seen anyone doing network exploitation through application updates before.

tochk0 - July 8, 2019, 8:32 am

That sounds good, I am not so experienced YET, but isn't that similar to the router firmware update? Correct me if I am wrong, please.

Jacque Fresco - July 8, 2019, 9:59 am

Sounds pretty doable. It would probably be needed to sniff the Network for a while to get a clue which Program the target has actually installed (that searches for updates on the net). Having a list of Programs the Attacker could now try to inspect the Programs and tamper around to see what results he get (the less developed or the younger a program is the higher the chance is that the Update process is under developed).

This Method does not need, like the "Replace what ever the User downloads" Method, a Users Verification and can be done even when the User is not on the Computer, since Updates are being Searched on alot of Programs in the Background.

Like the Brave Browser where the Update Search runs every Hour and on Logon.

If we analyze enough how the Updating works on what ever Program we may even dont need to wait until a Real Update is being release to replace it. We could simulate with MITM or what ever that we are the Server and that a Update is being available.

(Jul 8, 2019 09:56 AM)CyberStrike Wrote: [\[CITE\]](#) [Not an actual Quote]

I hope you dont mind, i believe this is your Area of Expertice. What do you think about Mr. Robots Idea?

CyberStrike - July 8, 2019, 10:21 am

ISR-EvilGrade does this already, using something like bdf-proxy you can backdoor downloads on the fly, now code signing certs will be needed. Some browsers (eg Chrome) has an extensions using ESET scanner, which I believe it checks sha256sum perhaps sha1. There are some applications which update over http still actually.

Jacque Fresco - July 8, 2019, 11:05 am

(Jul 8, 2019 10:21 AM)CyberStrike Wrote: [\[CITE\]](#) ISR-EvilGrade does this already, using something

like bdf-proxy you can backdoor downloads on the fly, now code signing certs will be needed. Some browsers (eg Chrome) has an extensions using ESET scanner, which I believe it checks sha256sum perhaps sha1. There are some applications which update over http still actually.

Thank you for your Response ?

I dont know a Application that uses the Browser to Update. They do that them self. So the Scanner would be no Issue. So in case there is a Program actually Retrieving Update Information (may even the update itself) over this unsecure Connection, anyone could actively Manipulate the Transmitted Data. Thats interesting.

[infobyte/evilgrade](https://infobyte.github.io/evilgrade)

CyberStrike - July 9, 2019, 6:41 am

(Jul 8, 2019 11:05 AM)Jacque Fresco Wrote: [\[CITE\]](#) Thank you for your Response ?

I dont know a Application that uses the Browser to Update. They do that them self. So the Scanner would be no Issue. So in case there is a Program actually Retrieving Update Information (may even the update itself) over this unsecure Connection, anyone could actively Manipulate the Transmitted Data. Thats interesting.

[infobyte/evilgrade](https://infobyte.github.io/evilgrade)

Well if it's your own rogue AP you can get away with quite a few things which probably normally wouldn't be possible in the average network. I am pretty sure one can develop their own modules where it's predicated upon running a rogue AP.