

Forum:[Hack Forums](#)

Thread: [RAT's, Ransomware, Remote Access \(Discussion\)](#)

Oldylox1 - June 25, 2020, 9:27 pm

So I've been playing around with RAT's and crypters for a while now on my VM, just purely out of curiosity and for more of a prevention for the future within my own company.

A little background:

A customer of ours got hit by a Ransomware attack a few weeks ago, which ended up causing them to have a 3 day downtime due to having us restore everything (Full OS reinstalls on 5 servers and 6 computers).

What I found:

Interestingly enough as I investigated it, the entrypoint appeared to be directly on one of the directors computers. Whilst Symantec is what we use for all of our customers rather than a FUD runtime breach it appears what has happened is the culprit used Aterra RMM to compromise his system.

Firstly, Aterra RMM after further investigation (A trial package) is quite useful software, but from a IT security perspective appears to just have loopholes everywhere.

With Aterra, you have full access to the PC, it is a complete silent install so the user does not know unless they look in Programs and Features, which in realworld a normal corporate user will not do that often.

They have installed Aterra and used its Command prompt (Elevation) feature to net user password reset, uninstall Symantec, and finally run their Ransomware. Although it appears at first they used AsyncRAT to password recovery everything they could (as 30 of the customers personal saved passwords for websites were used on those accounts/attempted logins), then ran their ransomware.

The concerning thing with RMM's these days, is they use Splashtop as an example for Remote Desktop. Now, by standard if you went and purchased Splashtop business, it prompts the end computer if they trust <company name> to install this and warns them of what the company can do to their PC, however with RMM's it is a complete silent install, and you have an option to black out the screen and block any input.

Aterra also has a WAKE ON LAN feature which was used in this instance.

We still cannot find out how Aterra was installed on the computer in the first place, it may have been binded with a legitimate file I assume. However, the culprit has been arrested. (He used his real name on his Aterra account when he signed up, also paid with his bank card).

So what I wanted to figure out is, obviously going forward we will be moving to another AV provider.

My Question:

I have recently been getting a FUD runtime and scan via Windows Defender with RAZ Private stub alongside Hive Rat, Warzone Rat, BitRAT and AsyncRat.

Got my hands on a corporate edition of ESET trial, and also home edition but what is quite interesting is that scanning these files reveal nothing malicious, but ESET seems to be quite aggressive and does pickup on runtime that these are trojans/variants.

On runtime ESET is detecting: "MSIL/Agent.TWO Trojan"
On Password recovery in all RATS ESET detects: MSIL/Injector."UWL Trojan" & :
"Generik.DVCZOHP Trojan" then with VNC it detects "Agent.CTE"

So to further my curiosity, has anyone/does any current crypter/RAT bypass ESET at all or have know of any methods to bypass this?
it seems they are doing a very good job in terms of detecting RATS/Malicious software which is a bonus for us.

We have started using RMM now (funnily enough, Aterra), which allows us to set instant email notifications of uninstalling of applications, suspicious activity etc (Which I have, rest assured FULLY tested to my hearts content on one of our spare computers in our office).

So, uninstalling of AV in a perspective of the above scenario should flag up to us now.

Is there any AV companies out there that prevent any uninstalls of their AV without just say, a master password (Rather than Admin rights).

Thanks!