

## Forum:[Hack Forums](#)

Thread: [Anyone notice the article "RAT Vulnerabilities Turn Hackers into Victims"](#)

**Ghostzapper** - June 24, 2017, 9:08 am

I was wondering what the users and makers of RATs think about this article.

The article is on DarkReading.com and is about Gh0stRAT, Korplug/Plug-X, and XtremeRAT, among others. The article which is reporting on a talk called "Digital Vengeance: Exploiting the Most Notorious C&C Toolkits" at the BlackHat USA 2017 conference.

Basically it says: The command-and-control components of these tools have vulnerabilities that can be exploited by attacker targets, who can turn the tables on their assailants.

"The attacker who was the attacker is now the victim," says Grange(the speaker at the conference) of the exploits' capabilities, which could enable a target to remote into an attacker's machine and browse it. "The tools can expose them to more vulnerabilities than the people they're targeting in some ways."

By using a python script Grange said about Gh0stRAT:

"It's fairly easy to recognize," says Grange. "Most antivirus products pick it up right away because it has been around for so long."

If a machine's antivirus program discovers the Gh0stRAT component, he continues, people have developed a Python script to search the malware and pull out configuration information. This script can "call home" to the C&C address and provide data on the adversary's location.

Armed with the location of the attacker's server, a victim can install malware back on the adversary's machine and view their screen and files.

"I can see who the adversary has as their targets," says Grange. "If they're remote controlling someone else, I can see what connections they have to others; what files they may have gotten off other targets."

Any thoughts about this?

**QU?CKSILVER** - June 24, 2017, 9:29 am

Indeed, there are a few vulnerable RATs that can be exploited by targeting the port they're listening on. DarkComet is another example of this. RATs around here are probably vulnerable too, it's just that nobody has dug deep enough to find vulnerabilities in those CnCs that could allow remote code execution, or the discoverers are keeping it a secret.

I'm still waiting for the day an exploit for a popular RAT gets leaked. Many security researchers and cyber criminal hunters will benefit from this.

**Ghostzapper** - June 24, 2017, 10:33 am

Quicksilver your insights are probably right. I wonder what some of makers of RATs who are selling them here on HF have to say about how they would protect buyers from this vulnerability...or if they have figured out a way. Also, I wonder what the Python code would look like....if there are any Python experts reading this thread.

**TheWarOwl** - June 24, 2017, 10:37 am

There's always going to be some kind of "offensive" hacking. Where someone fights back against malicious use. I'm sure there's plenty of 0 days that effect common RAT's.

It's just a matter of time until certain vulnerabilities are disclosed.

**Purple Kief** - June 24, 2017, 2:17 pm

(Jun 24, 2017 10:33 AM)Ghostzapper Wrote: [\[CITE\]](#) Quicksilver your insights are probably right. I wonder what some of makers of RATs who are selling them here on HF have to say about how they would protect buyers from this vulnerability...or if they have figured out a way. Also, I wonder what the Python code would look like....if there are any Python experts reading this thread.

Don't forget you are looking at software that was coded ages ago.  
Current (paid) RAT developers are updating their software, and they're more aware of vulnerabilities than this than any of us are. ?

**Batzii** - June 24, 2017, 3:14 pm

Don't get a free rat problem solved

**Hatchet** - June 24, 2017, 4:16 pm

(Jun 24, 2017 03:14 PM)Batzii Wrote: [\[CITE\]](#) Don't get a free rat problem solved there we go ? some one with a juice !

**#Skyline** - June 24, 2017, 6:44 pm

(Jun 24, 2017 02:17 PM)Purple Kief Wrote: [\[CITE\]](#) Don't forget you are looking at software that was coded ages ago.

Current (paid) RAT developers are updating their software, and they're more aware of vulnerabilities than this than any of us are. ?

False.

Could be 0days.

Just an example, current employees of Microsoft are updating there software/OS's regularly, but recent past events tell us Microsoft wasn't aware of the SMB vulnerability that allow the usage and spread of WannaCry, only intelligent agencies knew and had access to use it, until it got leaked.

So what I am saying is, they're vulnerabilities we don't even know about.

So don't trust a RAT dev, who cares if they're your friend or a member of the forum or not. You're always gonna take risk.

**Purple Kief** - June 24, 2017, 7:12 pm

(Jun 24, 2017 06:44 PM)#Skyline? Wrote: [\[CITE\]](#) False.  
Could be 0days.

Just an example, current employees of Microsoft are updating there software/OS's regularly, but recent past events tell us Microsoft wasn't aware of the SMB vulnerability that allow the usage and spread of WannaCry, only intelligent agencies knew and had access to use it, until it got leaked.

So what I am saying is, they're vulnerabilities we don't even know about.

So don't trust a RAT dev, who cares if they're your friend or a member of the forum or not. You're always gonna take risk.

I mean you pretty much say it yourself..

You can't trust anything, but people still download stuff regardless of that, it's how the internet

works.

Bottom line remains, get a paid RAT that is updated regularly and you should be fine.

**QU?CKSILVER** - June 24, 2017, 7:33 pm

(Jun 24, 2017 06:44 PM)#Skyline? Wrote: [\[CITE\]](#) recent past events tell us Microsoft wasn't aware of the SMB vulnerability that allow the usage and spread of WannaCry,

Somebody told them earlier and patched it before the leak. Still wondering if the NSA told Microsoft about it before the chaos.

**yotoprules** - June 25, 2017, 4:41 am

You can also use a virtual machine or a crappy laptop to do the job.

**loadman** - June 26, 2017, 12:09 pm

(Jun 24, 2017 06:44 PM)#Skyline? Wrote: [\[CITE\]](#) False.

Could be 0days.

Just an example, current employees of Microsoft are updating there software/OS's regularly, but recent past events tell us Microsoft wasn't aware of the SMB vulnerability that allow the usage and spread of WannaCry, only intelligent agencies knew and had access to use it, until it got leaked.

So what I am saying is, they're vulnerabilities we don't even know about.

So don't trust a RAT dev, who cares if they're your friend or a member of the forum or not. You're always gonna take risk.did Microsoft knew about the loophole and they didn't patch so that NSA could use it? coz I'm sure they cant be that stupid to not fix that. idk maybe I'm wrong