

Forum:[Hack Forums](#)

Thread: [\[TUT\] Explaining Keyloggers and RATs!](#)

Brado - June 23, 2014, 6:35 am

Here a few information about Keyloggers and RATs.. And the differences between this two!

If you want to use one of those two.. I would advice you to buy one! Cause they are much better and easy to use! If you want to use a Free RAT tool, i recommend you to use Darkcomet([Click here](#))!

Keyloggers & RAT's: [Click here](#)

Keyloggers ([Click here](#))

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. It has uses in the study of human-computer interaction. There are numerous keylogging methods, ranging from hardware and software-based approaches to acoustic analysis.

These are computer programs designed to work on the target computer's software. From a technical perspective there are several categories:

Hypervisor-based explanation: [Click here!](#)

Hypervisor-based: The keylogger can theoretically reside in a malware hypervisor running underneath the operating system, which remains untouched. It effectively becomes a virtual machine. Blue Pill is a conceptual example.

Kernel-based explanation: [Click here!](#)

Kernel-based: A program on the machine 'gets root' and hides itself in the OS, and starts intercepting keystrokes (because they always go through the kernel). This method is difficult both to write and to combat. Such keyloggers reside at the kernel level and are thus difficult to detect, especially for user-mode applications who don't have root access. They are frequently implemented as rootkits that subvert the operating system kernel and gain unauthorized access to the hardware, making them very powerful. A keylogger using this method can act as a keyboard device driver for example, and thus gain access to any information typed on the keyboard as it goes to the operating system.

API-based explanation: [Click here!](#)

API-based: These keyloggers hook keyboard APIs inside a running application. The keylogger registers for keystroke events, as if it was a normal piece of the application instead of malware. The keylogger receives an event each time the user presses or releases a key. The keylogger simply records it.

Windows APIs such as `GetAsyncKeyState()`, `GetForegroundWindow()`, etc. are used to poll the state of the keyboard or to subscribe to keyboard events. A more recent example simply polls the BIOS for pre-boot authentication PINs that have not been cleared from memory.

Form grabbing based explanation: [Click here!](#)

Form grabbing based: Form grabbing-based keyloggers log web form submissions by recording the web browsing on submit events. These happen when the user finishes filling in the form and clicks on the "OK" or "Submit" or "Go" or anything that indicates that you're finished. This records form data before it is passed over the Internet. .

Memory injection based: Memory Injection (MitB)-based keyloggers alter memory tables associated with the browser and other system functions to perform their logging functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors who are looking to bypass Windows UAC (User Account Control). The Zeus and Spyeye Trojans use this method exclusively. Non-Windows systems have analogous protection mechanisms that need to be thwarted somehow by the keylogger.

Packet analyzers explanation: [Click here!](#)

Packet analyzers: This involves capturing network traffic associated with HTTP POST events to retrieve unencrypted passwords. This doesn't work if you're connected with HTTPS - in fact it was this kind of attack they were fighting when they invented HTTPS.

Remote access software keyloggers

These are local software keyloggers with an added feature that allows access to the locally recorded data from a remote location. Remote communication may be achieved using one of these methods:

- Data is uploaded to a website, database or an FTP server.
- Data is periodically emailed to a pre-defined email address.
- Data is wirelessly transmitted by means of an attached hardware system.
- The software enables a remote login to the local machine from the Internet or the local network, for data logs stored on the target machine to be accessed.

Most of these aren't stopped by HTTPS encryption because that only protects data in transit between computers; this is a threat in your own computer - the one connected to the keyboard.

[Wikipedia](#)

RAT's ([Click here](#))

A remote administration tool (a RAT) is a piece of software that allows a remote "operator" to control a system as if he has physical access to that system. While desktop sharing and remote administration have many legal uses, "RAT" software is usually associated with criminal or malicious activity. Malicious RAT software is typically installed without the victim's knowledge, often as payload of a Trojan horse, and will try to hide its operation from the victim and from security software.

The operator controls the RAT through a network connection. Such tools provide an operator the following capabilities:

- Screen/camera capture or image control
- File management (download/upload/execute/etc.)
- Shell control (from command prompt)
- Computer control (power off/on/log off if remote feature is supported)
- Registry management
- Hardware Destroyer

- Other software product-specific functions
- Its primary function is for one computer operator to gain access to remote PCs. One computer will run the "client" software application, while the other computer(s) operate as the "host(s)".

Contents

- 1 RAT trojan horses
- 2 Notable RAT software and trojans
- 3 See also
- 4 References

RAT trojan horses

Many trojans and backdoors now have remote administration capabilities allowing an individual to control the victim's computer. Many times, a file called the client must be opened on the victim's computer before the trojan can have access to it. These are generally sent through email, P2P file sharing software, and in internet downloads. They are usually disguised as a legitimate program or file. Many server files will display a fake error message when opened, to make it seem like it didn't open. Some will also disable antivirus and firewall software. RAT trojans can generally do the following:

- Block mouse and keyboard
- Change the desktop wallpaper
- Download, upload, delete, and rename files
- Destroy hardware by overclocking
- Drop viruses and worms
- Edit Registry
- Use your internet to perform denial of service attacks (DoS)
- Format drives
- Grab passwords, credit card numbers
- Hijack homepage
- Hide desktop icons, taskbar and files
- Install software
- Log keystrokes, keystroke capture software
- Open CD-ROM tray
- Overload the RAM/ROM drive
- Print text
- Play sounds
- Control mouse or keyboard
- Record sound with a connected microphone
- Record video with a connected web cam
- Show fake errors
- Shutdown, restart, log-off, shut down monitor
- Steal passwords
- View screen
- View, kill, and start tasks in task manager

A well-designed RAT will allow the operator the ability to do anything that they could do with physical access to the machine. Some RAT trojans are pranks that are most likely being controlled by a friend or enemy on April Fool's Day or a holiday. Prank RATs are generally not harmful, and won't log keystrokes or store information about the system on the computer. They usually do disruptive things like flip the screen upside-down, open the CD-ROM tray, or swap mouse buttons.

[Wikipedia](#)

Linker - June 23, 2014, 7:09 am

Thank you so much! Wish I could +1 this! You are gonna help so many people with this good job man!

:D

Eddie-Venom - June 23, 2014, 7:11 am

Thanks for this Black Label, very well presented and very informative.

Brado - June 23, 2014, 7:19 am

Thanks for the review guys.. Appreciate it!! And i also hope that this will help some people out!

Niely - June 23, 2014, 7:25 am

Nice explanation of all! :)

For sure the one of key-loggers. ;)

Keep on the good work!

Brado - June 23, 2014, 7:28 am

(Jun 23, 2014 07:25 AM)Niely Wrote: [\[CITE\]](#) Nice explanation of all! :)

For sure the one of key-loggers. ;)

Keep on the good work!

thnx bud. It would be great if this help some peeps out?

UkVenoM - June 23, 2014, 7:31 am

Great post! I havnt seen anyone go into all the different methods before nice work! ?

Nutrition - June 23, 2014, 7:32 am

Great post, looks like a lot of time was put it! HQ.

Brado - June 23, 2014, 7:33 am

(Jun 23, 2014 07:31 AM)UkVenoM Wrote: [\[CITE\]](#) Great post! I havnt seen anyone go into all the different methods before nice work! ?

Thnx bro. Yes here are all the properties discussed.

(Jun 23, 2014 07:32 AM)Bit Bucket Wrote: [\[CITE\]](#) Great post, looks like a lot of time was put it! HQ.
Thnx! No not so much time haha.

Eddie-Venom - June 23, 2014, 7:43 am

So lets say I purchase a crypter and when tested the file is FUD, in a month or so the 'slaves' AV will pick it up and I'll randomly lose a victim from my list unless i keep updating the file to remain FUD?

Or once the file is on the victims machine it will remain FUD?

Brado - June 23, 2014, 7:52 am

(Jun 23, 2014 07:43 AM)Eddie-Venom Wrote: [\[CITE\]](#) So lets say I purchase a crypter and when tested the file is FUD, in a month or so the 'slaves' AV will pick it up and I'll randomly lose a victim from my list unless i keep updating the file to remain FUD?

Or once the file is on the victims machine it will remain FUD?

That depends on your victim.. If he knows that he's infected he will remove it by himself. Otherwise when you infect him with a FUD stub and he observes nothing of it, he will stay on. When his av detect your stub as a virus it will remove the file. If the owner gives the AV permission to do it.

Private Network - June 23, 2014, 8:22 am

Good explanation, This would have helped me when i was a noob :P

Brado - June 23, 2014, 8:39 am

(Jun 23, 2014 08:22 AM)JesseTheLegend Wrote: [\[CITE\]](#) Good explanation, This would have helped me when i was a noob :P

Haha you are already grown up in this world!

swagster1337 - June 23, 2014, 3:24 pm

Super high quality thread :)

Thank you very much for the useful information

Appreciate it bro.

Cletus Kasady - June 23, 2014, 3:58 pm

Very nice thread. I always like seeing a high quality thread in this forum, it gets annoying going on threads like 'help me hax ma cheating bf faceboak'.

Brado - June 23, 2014, 4:08 pm

(Jun 23, 2014 03:24 PM)swagster1337 Wrote: [\[CITE\]](#) Super high quality thread :)

Thank you very much for the useful information

Appreciate it bro.

Thnx bro! Love to hear this!

(Jun 23, 2014 03:58 PM)Cletus Kasady Wrote: [\[CITE\]](#) Very nice thread. I always like seeing a high quality thread in this forum, it gets annoying going on threads like 'help me hax ma cheating bf faceboak'.

Thanks buddy! Yes indeed threads like that are very annoying.. This thread is at least something that will help people out!

Cletus Kasady - June 23, 2014, 4:10 pm

(Jun 23, 2014 04:08 PM)Black Label™ Wrote: [\[CITE\]](#) Thanks buddy! Yes indeed threads like that are very annoying.. This thread is at least something that will help people out!

Yeah hopefully this will of reduced the need for a few of those posts.

Brado - June 23, 2014, 4:14 pm

(Jun 23, 2014 04:10 PM)Cletus Kasady Wrote: [\[CITE\]](#) Yeah hopefully this will of reduced the need for a few of those posts.

Yes i hope it also. But yeah unfortunately some people are to lazy to search for something..?

LampShed - July 12, 2014, 8:00 am

Could you at all explain how to make a RAT? Awesome thread would love to see more of these ?

... it makes me happy ???

????ll?? - July 12, 2014, 10:14 am

thx im gonna use this guide :)!!!!!!

Erwin Schrödinger - July 12, 2014, 10:15 am

I never fully understood a RAT virus, and this really helped me out!

Thanks! <3

Brado - July 28, 2014, 9:29 am

(Jul 12, 2014 08:00 AM)dr_peekaboo Wrote: [\[CITE\]](#) Could you at all explain how to make a RAT?

Awesome thread would love to see more of these ?

... it makes me happy ???

There are many RAT softwares on hf. Darkcomet is a good and free one! If you use one of those you need to portforward. Otherwise you can use a VPN/VPS.

(Jul 12, 2014 10:14 AM)Gritzy1 Wrote: [\[CITE\]](#) thx im gonna use this guide :)!!!!
Nice to hear that you like it!

(Jul 12, 2014 10:15 AM)Erwin Schrödinger Wrote: [\[CITE\]](#) I never fully understood a RAT virus, and this really helped me out!
Thanks! <3
It's nice to hear that it helped you!

JessyDyk - July 28, 2014, 2:33 pm
Nice post mate! Think this really helps a lot

Brado - September 9, 2014, 12:35 pm
(Jul 28, 2014 02:33 PM)JessyDyk Wrote: [\[CITE\]](#) Nice post mate! Think this really helps a lot
Thanks buddy for saying! I also hope it will help people out!

Hassan Gazi - October 3, 2014, 2:57 am
A very great thread. Thanks a lot for making this :) Would love to learn more about this RATs. Asked few questions, please answer as soon as possible. Thanks a lot in advance ?

MDL00t - October 3, 2014, 10:35 am
nice one man, very in depth explanations!
salute,
-L00tr

hacipa - October 3, 2014, 4:38 pm
This is awesome. Exactly what I was looking for, I was going in circles before this. :) Very helpful!

macuna22 - October 3, 2014, 4:45 pm
this was really helpful man, thnx alot i bookmarked for future reference haha

Anodise - October 3, 2014, 5:01 pm
Nice guide OP, taught me a couple of things. Thanks.

Vextoray - October 3, 2014, 5:29 pm
I really enjoyed this tutorial, I didn't know most of these keyloggers. Thanks for providing a myraid of links and great and simple explanations!

Best regards.

Fudster - October 3, 2014, 9:52 pm
This tutorial is really nice. just ing this so others can see it.

LeGiT bK - October 3, 2014, 10:12 pm
Great tut! Very helpful and very HQ!
Thanks a lot!

Doxicity - October 3, 2014, 10:14 pm

This was a very nice tutorial for new users. Many RATs do offer the features he listed, and even more too.

Hopefully many more will see this.

Brado - *October 4, 2014, 12:08 am*

Thanks everyone! Love to hear that you guys like it!

Bo Burnham - *February 27, 2015, 12:01 am*

Guide was extremely easy to follow and noob-friendly, thankyou.

Romario - *February 27, 2015, 12:10 am*

Great post it's explained perfectly.

p.s: your signature it's provocative lol

fed1 - *February 27, 2015, 5:19 am*

Thnx bro! ?????

Vuln - *February 27, 2015, 5:29 am*

Great contribution OP.

(Jun 23, 2014 06:35 AM)Black Label™ Wrote: [\[CITE\]](#) Many times, a file called the server must be opened on the victim's computer before the trojan can have access to it.

Tiny common mistake there, you're confusing the server with the client.

See also <https://hackforums.net/showthread.php?tid=4695132&page=2>

Brado - *March 2, 2016, 4:05 pm*

Maybe this thread can still help some people out.

If you have any question you can always send me a PM!