

Forum:[Hack Forums](#)

Thread: [Remote Admin Tool 101 Course - Written By: Armada](#)

Armada - September 18, 2015, 11:24 pm

Written By: [A?mªĐa](#)

Project Status: Complete

Table of Contents:

Section 1: My First Pet R.A.T.

Spoiler ([Click to View](#))

Section Complete [1.1 Central Network Communication](#)

-- Advanced Knowledge - [IPv4](#) / [OSI Model](#)

[1.2 Picking the right R.A.T. for you](#)

-- Additional Reading: [Hacker Riskware](#)

[1.3 Networking from a Remote Administrative Point of View.](#) (R.A.T. POV)

- [Windows Firewall](#)

[1.4 Install and Configuration of your R.A.T.](#) - Covers Install and Configuration of Luminosity Link

1.2 and Imminent Monitor 3

- Official Guides: [Nanocore RAT](#) / [Babylon RAT Setup and Config](#) / [Babylon C++ RAT #2 #2](#) / [Luminosity Link Resources LL Setup Guide](#) / [Imminent Monitor 3 Tutorial Videos](#)

- User Guides: [Dark Comet](#)

Section 2: Health and Safety

Spoiler ([Click to View](#))[2.1 - R.A.T. Health and Safety](#)

[2.2 - Controllers Security Principals](#)

[2.3 - Clients Security Precautions](#)

Change Log:

Spoiler ([Click to View](#))

Code 2015-07-28

- Post 2.1

- Post 2.2

2015-07-26

- Section 2 defined in chapter course.

2015-07-23

- Post 1.4

2015-07-21

- Post 1.3

2015-07-18

-Post Central Thread

- Post 1.1

- Post 1.2

Armada - September 18, 2015, 11:25 pm

Written By: [A?mªDa](#)

[Main Course Thread](#)

Introduction:

When we discuss Networking and Network topologies on a Remote Administration and associated technology level. A new array of problems and configuration concerns must not only be met, but also carefully configured to not compromise security to the designated user. This being said, we need to look at and approach networking in a different perspective to start. Where most users when they begin in the network security field believe they already have a good understanding of basic networking because they can hook up a cable modem and wireless router without issue. Remote Administrative tools require special and unique network configurations to ensure correct and proper communication.

The Basics, without being so basic.

Spoiler ([Click to View](#))

Figure 1 – 2 Computers in Communication.

In this model we have the simplest figure of computer networking. 2 machines in direct communication using a form of networking protocol (Likely IPv4 or IPv6). In this model the computers are shown with no protective measures, firewalls or anti-virus/security protection software elements in place. – A scenario now a days which is highly unlikely.

Figure 2 – 2 Computers in Communication with Firewall/Security in Place.

In Figure 2 we examine a more likely scenario where a computer has running security provisions in place. – In this example a firewall is in place on machine #1 – This scenario allows for machine #1 to accept requested information, send information outbound, however restrict unauthorized communication from machine #2, or other machines which may attempt communication.

Understanding your networks security provisions will greatly reduce troubleshooting of connectivity problems later on.

Every layer in the network has the potential to have another form of network security in place. It is highly recommended before attempting to start use of Remote Administrative tools the user sit down and plan the networks design and strategy out beforehand. Use of Microsoft Visio is a fantastic resource for such network planning.

Figure 3 – A Typical Home Network Design

In Figure 3 we have a Typical Home Network design, with common elements of network connectivity. A Cable Modem (Or DSL) which provides the network gateway and hardware interface for the communication. The Wireless Router which provides resource sharing of the modems internet connectivity, and the various devices used to access the network.

However, there are hidden or less known layers which also exist within even the simplest of networks such as detailed in figure 3.

Figure 4 – Detailed Typical Home Network Design

In Figure 4 we examine a more detailed, but “same” network configuration. Just with a more accurate view of possible network boundaries.

Each device presents its own unique security boundaries and configurations. Workstation and Laptop terminals employ software/OS firewall security and likely Anti-viral software. Network peripherals such as Routers and Modems (or Combo devices) also present firewalls which are hardware based and accessed through the devices interface (Likely a web browser accessible configuration page). Each and Every device and security measure along the network path/route from the Internet WAN to the device being used by the user to access such Remote Administrative tasks MUST BE CORRECTLY configured to allow the network traffic to pass. In more complex networks, this can become especially tricky for some users if they do not have the correct network privileges or rights to modify the required settings.

Network Exercise:

Spoiler ([Click to View](#))

Creating a basic network flow/layout.

Users are encouraged to sit down, and record each and every device connecting their network together. This includes finding the make and model of every network peripheral included.

Although this varies from ISP and network configuration greatly, it is in general safe to assume a user with High speed internet will have the following:

Cable Modem: (Make/Model)

Wireless/Wired Router: (Make/Model)

Various Terminals/Computers: (Make/Model/OS Version/Security In Place)

Record each devices model and serial and find on the manufacturers website is that devices model enforces security measures.

For Modems and Routers firewall configurations are essential to PORT FORWARDING.

Routers being the general devices to provide resource sharing across a network will be the Default Gateway for most devices (and thus easily accessed by using gateways IP# in the browser to access the configuration page) It is important to understand that every devices layout and options will vary to a degree from model to model. So it is highly recommended to sit down, record your settings for each device and familiarize yourself with the configurations layout and settings pages are, and where features are located.

Finding your default gateway:

In Windows Navigate to your Command Prompt

Start > Run > type “cmd”

In Command Prompt type “ipconfig”. The user will be prompted with a similar dialog reply:

C:\>ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : Home

Link-local IPv6 Address :

IPv4 Address. : 192.168.1.50

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.1

The listed Default Gateway will likely be your internal Routers IP#. And also the network address in which the Routers configuration page and settings can be accessed (Through web browser interface).

// End Exercise

Port Forwarding:

Spoiler ([Click to View](#))

Majority of times more than others, the usual reason for a RAT failing to "work correctly" with new users is incorrect port forwarding rules. Without going in to too much detail, the simplest way to explain port forwarding is, within the network a user generally has 2 IP#'s. One Internet based IP# (Which is the users physical address on the internet) and a local LAN IP# (usually named 192.168.*.* or similar depending on router model.) When a user opens a port for external network communication from the internet, the port must then be pointed to the correct Local Area Network IP# (The 192.168.*.*) For this reason a user who is dealing with port forwarding is recommended to make the machines local IP# static to it does not change within the local area network, and prevents further problems with port forwarding.

This can be accomplished by accessing the Local area connection in the Control Panel of Windows > Network and Sharing Section > Change Adapter Settings.

Right clicking on the active adapter and selecting Properties > Internet Protocol version 4 > Properties.

"Use the following IP address"

- Specify a valid local subnet IP# (I recommend something like 192.168.1.121, .121 as it is high enough in the IP# pool to not be assigned on a regular basis by dynamically addressed devices.) Subnet mask can almost always be left as the default.
- Default Gateway is the Routers IP#. (If you are a 192.168.1. IP#, Router is usually 192.168.1.1)
- Primary DNS server is ALSO the routers IP#.

- If configuration does not work, or internet connectivity is lost after attempting these steps, reassign IP# to "Obtain IP address automatically" to restore connectivity.

Verification of active R.A.T. port:

A simple way to verify the service has been executed successfully on the machine to be the slave is to run the netstat command from the terminals command line and look for the defined port in the listing.

Local Address - Is the local loopback (127.0.0.1 and the port number active from obviously, the local machine.

Foreign Address - Is the remote machine in which the connection is taking place with. (Command and Control, for example)

If you do not actively see the R.A.T.s defined port either communicating out, or alternatively (Command and Control Side) actively listening on the port, communication between client and

server will fail.

Router Configuration for Port Forwarding:

Spoiler ([Click to View](#))

Router configurations vary in layout, but all routers contain a feature for "Port Forwarding". This is where you can tell the routers hardware firewall to allow remote connectivity in to your network. This is essential for ANY R.A.T. or software with "Call home" functionality. Within the routers configuration you must locate the Port forwarding section and add an exception for the Port number you assigned in your R.A.T.s configuration. This port must then be forwarded to a local IP# within your network (The workstations IP# you will be using the command and control from)

RAT101 1.1 - v.1

Armada - September 18, 2015, 11:26 pm

Written By: [A?m^aDa](#)

[Main Course Thread](#)

Selection, oh the selection!

When it comes to the users final selection on software there never is a single "go to". This put simply is left to the users determination on their personal needs. For all intensive purposes we are going to assume straight forward remote admin tool.

We want a base line of the following functionality:

Spoiler ([Click to View](#)) Remote file directory listing upload/download

Remote keylogging

Password Management

File Search / Indexing

Remote Desktop and or Webcam

Consideration to the free:

Spoiler ([Click to View](#))

[njRAT 0.7](#)

Arguably one of the best free RATs available. No Authentication server means no risk of remote take over. standard features, however limited support.

[Dark Comet](#)

A well known and highly recommended RAT offered freely, however due to its success now has known flaws and open exploits not patched by typical public versions. Use with care and caution.

[xRAT](#)

Stability and Simplicity in a single package. This RAT offers both with absolute reliability. Source code is offered freely, so programmers can freely modify at will to best tailor to their personal needs.

When free is no longer viable, its time to look at paid for solutions:

Spoiler ([Click to View](#))

[Luminosity Link](#)

Key Features: Remote System Surveillance

File Management and File Search
Keylogging
Password Management and Recovery
Anti-Malware
Reverse Proxy
Integrated CryptoMiner
Ring3 Rootkit
Key Drawbacks: Controllers Interface can be laggy
Host binary can be unstable at times
File Management can stop responding

[Imminent Monitor 3](#)

Key Features: Remote Surveillance
Remote File Management
Reverse Socks Proxy
Plugin System
Anti-Malware
Integrated CryptoMiner
Visual Connections Map
Torrent Seeder
Key Drawbacks: File transfer can cause corruption
Binary instability can cause loss of host machines
"Troll" features can be hard to resist (hehe...)

[NanoCore](#)

Key Features: Remote File Management
Remote Desktop and Webcam
Extensive Plugin System
Network and System Management
Remote Registry Editor
Remote Command Console
Scripting management Interface
Port Management \ Advanced Network Control
Key Drawbacks: Some functionality can be buggy depending on host system configuration
Escalation of privilege feature can cause instability in binary

[OSCelestial RAT](#)

Key Features: Undetected by security software
Java based application giving ability to run on different operating environments.
.jar injector
Password Management \ Recovery
Key Drawbacks: Java based appliance causes instability

It is important to note that there are numerous other Remote Administrative Tools both Paid and Free. Too many to list entirely.

Want additional user input on the various Remote Admin Tools?

[Check Out THIS Article](#)

Picking the right R.A.T. for your needs:

Spoiler ([Click to View](#))

First, I need to explain something when it comes to Remote Administrative Software.

When it comes to Remote Administration, functionality and reliability are KEY. Everything else comes secondary.

This being said it is MORE important to focus on your requirements to management rather than the price tag associated to the solution.

The end administrator and R.A.T. controller needs to determine some very specific scope guide lines before making a decision on a solution.

some recommended guide lines are as follows:What is the scope of the network project? How many hosts are planned for the project?

What administrative control is required for the hosts?

What security considerations are to be implemented or considered/observed?

How long will the project run for and/or how long will the Remote Admin Tools remain on the host machines?

These base lines and the administrators own considerations must be closely examined and every Remote Administrative tool must be closely analyzed to compare and determine the "Best Fit".

Key considerations are per network build. and greatly vary too much to accurately advise on.

When it comes to Hacker Networks, deal with the Known and trusted. Within the community there are numerous highly qualified members whom offer such services or Help desk services bot free and paid.

FREE vs. PAID

Spoiler ([Click to View](#))

At this point after we have determined what requirements are needed for our uses.

It is now time to compare the Free and Paid for solutions against one another and determine which is the best solution for you.

In this degree, I argue the following:Is this a past time, or is there a very specific ambition to accomplishment?

How much time are you willing to invest in your R.A.T. project.?

Free:

The obvious here, is the solution is free. However the primary downside is it is all user based support basically.

Paid for solutions:

Paid for solutions come with the massive bonus of user support usually from the developers or a assigned approved support team whom can fix/correct the most common problems. The down side to paid for licensing to software such as this is the very possible likelihood of authoritative problems.

[Case Example of Black Shades](#)(Hacker Riskware)

Understanding your specific requirements, the security elements to protect not just yourself, the host machines and others whom might have involvement in Remote Administration are all potential target to numerous "less than savory types" - More on this later.

It is in this sections wrap up, where I leave the reader this question.

Which R.A.T. best suits your needs?

- Placing aside financial cost, which of the solutions you looked in to is best suited your needs?

It is this answer in which you are best to place focus on and obtain the correct software from the start.

- Understanding your needs best suits your final decision. Passive users whom just wish to "play around" with the networking concept, I personally would argue save your money, and go with a free solution to experiment. Those more serious will see the obvious benefit of a paid for solution, but must also understand the inherent risk associated with authentication services and databases which are held. - regardless of how minimal it may be.

RAT101 1.2 v.1

Armada - September 18, 2015, 11:27 pm

Written By: [A?m^aDa](#)

[Main Course Thread](#)

To begin in this chapter.

Spoiler ([Click to View](#)) I need coffee. F%*^ you brb

We examine a "A-typical" network configuration. Call it home diagram #1

But my network is different

- Of course it is. All networks will vary in design.

Call Home, Host, Clients, The R.A.T. Definition Guide.

Spoiler ([Click to View](#))

To start with basic understanding. It is vital to recognize that there is a difference between Legitimate Remote Administrative Tools, And Hackers less than legit purposes. This being stated, I will ONLY cover the Remote Administrative process from an Administrative point of view.

These next chapters are going to be intensive, highly recommend anyone serious, pickup a notepad for notes ?

R.A.T.

Typically the referenced binary application to a client server suite, which is designed for remote administration.

Controller

The central interface the remote administrator utilizes to manage host machines, further majority of controller interfaces are inclusive of a inherent builder interface to creating host binaries.

Client

This, again is a host machine. It is running the desired software for remote administration.

DNS

DNS stands of Domain Name System/Service. In respect to RAT and Remote Administrative

needs, we rely on dynamic services, which can be readily updated.

Remote Admin - Back to basics.Spoiler ([Click to View](#))

We examine the Home network, and the first obvious situation consideration is the designation of a host controller.

For intensive purposes, I have labeled a laptop as "Hacktop"

- this will be our controller.

Keeping this as SIMPLE as plausible in this scenario. Bear with me while I attempt to visually describe this concept.

We select a terminal to play CONTROLLER In this instance, the laptop named "Hacktop"

At this point the remaining network devices are to be ignored for all intensive networking purposes.

- Assigning the terminal to static IP# addressing:

Armada, when is static internal addressing suitable?

- This answer varies. In general I would suggest this solution if the controller is less likely to be transported around or access the network from multiple or various network connection points.

Hacktop is now assigned a IPv4 interface of 192.168.1.50

[-How to statically assign IP addressing](#)

We now must look at the networking from the outside perspective.

- I have a controller I am suppose to speak to, but it resides within layers of security.

How do I communicate with it?

So lets start with the obvious

The end game is a Remote Administrative Binary must speak to the Host Controller. In this example "Hacktop"

Port Forwarding

Spoiler ([Click to View](#))

To understand your port forwarding requirements, you must first understand the network hardware that provides you internet connectivity.

Cable Modem / ADSL Modem

The Modem, either Cable or ADSL. (Depending in provider) is the central device which sends and receives the data signal transmission which provide the fundamental communication for network communication. Modems, typically do not have barriers implemented in them. (Firewall, DMZ or other appliance security conditions) These modems will almost certainly be the first of hardware peripherals to connect to the physical cable to the outside world.

Router

Routers either wired or wireless provide end users with the ability to take the single connection provided by the modem and allow multiple devices to utilize the same connection between the

various devices. This is accomplished by the routers packet handling abilities. Routers not only provide for internal network (LAN) configurations which are unseen by the outside world. But also present the typical first layer of security within a A-typical home network configuration. This also from a Remote Administration Point of View. Provides out first boundary and limitation to successful network communication between a host machine and the remote administrative controller.

Combo Devices

Combo devices although not necessarily an overly popular solution are still a reality in the network world. Combo devices such as cable modem\router bundle hardware are typically lesser known brands and usually contain their own security configurations. In these instances where users are faced with these devices it is best recommended to read the instruction manual for any information pertaining to port forwarding or hardware firewall applications which might be inclusive in the hardware's design.

Port Forwarding Basics:

Spoiler ([Click to View](#))

Regardless of the device used, all network appliances have a fairly typical Port forwarding interface. I mean you can only make the layout of the settings so unique. Thus regardless of model brand, all Port forwarding/Firewall configurations have a A-typical layout.

In this article we will take a quick look at Netgear and Linksys branded port forwarding screens

As is clearly visible by either configuration. Some typical elements exist:

Application\Service Name - The name you have given for the firewall exception - Name this something you will remember what it is, but not totally obvious either. (Don't call it Dark Comet for example, call it remote connectivity)

Port forward start and stop ports - This will typically be a single port instead of a range of ports. Unless of course you have chosen to run your service on a range of ports for management reasons, we will assume a single port for this article of Port 1337

Internal IP# - This is the designated machine's internal IP# within the user's LAN. This IP# will typically start with the numbers 192.168.xxx.xxx or 10.1.xxx.xxx

And Protocol - Users will want to select either BOTH UDP/TCP or only TCP communication for the type of protocol to be utilized.

Important Note on Port Forwarding and Internal IP#:

Routers will blindly pass traffic to the designated internally assigned IP# without question. This being said, the router assumes the administrator has correctly configured the port forwarding and does not check if the Internal IP# it has been directed to forward communication on is in fact a live responding IP#.

This being said, Internal LAN IP#'s are also generally considered dynamic IP#'s as well. What does this mean to the Remote Admin? as opposed to statically assigned IP#'s which will not change, dynamic IP#'s request a IP# from the router. The routing device then pulls a IP# from a pool of available IP#'s and gives it to the device. This IP# can change on a daily basis if the network sees a lot of devices connect and disconnect to it. It is for this purpose. If the controller's machine is not to move often or change networks on a regular basis. It is best recommended to consider statically assigning an internal IP# to avoid trouble shooting connectivity at a later time.

Recommended Testing Process

Spoiler ([Click to View](#))

For all intensive purposes, testing should be done with little to no limitations in place initially. All security software and appliances should be disabled and enabled one at a time retesting with every change made.

This eliminates confusion to where a problem might be residing. Enabling anti virus, firewalls and other security software all at one time and then wondering why the connection is failing is like giving someone 50 biological viruses and then wondering which one is causing the health problem to the person.

If testing suddenly fails after a specific application has been turned on or enabled, but tests correctly when that application is disabled, the problem clearly lies in that configuration somewhere.

This wraps up section 1.3 ?

Armada - September 18, 2015, 11:28 pm

Written By: [A?mªDa](#)

[Main Course Thread](#)

Luminosity Link (v.1.2)

Presented By: [LSDoom](#)

Step 1: Binary Settings Spoiler ([Click to View](#)) After starting LuminosityLink head over to the "Server Management" Tab and find "Client Builder"

Its important to enter the correct Dynamic DNS (Figure 1) and the correct port (Figure 2). Enter the port you forwarded through your router or VPN.

(I recommend using all settings within LuminosityLink, but that really depends on your crypter. Be sure to check that before building your stub.)

Step 2: Port Setup Spoiler ([Click to View](#))

Still under the "Server Management" Tab find "Connection"

Right click - Add New Port -> Enter the port you forwarded and click "Start Listenin". It is very important that you start listening to the port, or else you will not get any connections.

Step 2: Building the Binary Stub Spoiler ([Click to View](#)) Go back to the "Server Management" Tab and find "Client Builder"

Double check that all your settings are good, then click BUILD CLIENT BINARY

You have now setup LuminosityLink correctly and you are ready to crypt it and start spreading. If you port forwarded correctly and setup your Dynamic DNS you should now get connections when people execute your binary.

To see your connected clients head over to "Machine List"

Imminent Monitor 3

Presented By: [A?mªDa](#)

Step 1: Login and Load IM3 Controller Software

Spoiler ([Click to View](#))

On successful login, users will be presented with the controller interface:

Step 2: Controller Configuration

Spoiler ([Click to View](#)) Users are directed to navigate to the "Settings" tab of the IM3 controller:

Within the settings area, there are 2 TABS to take note of in the upper portion of the controllers window. "General" and "Ports"

- I recommend enabling port listening on startup.

Other options can be configured to administrators liking. (Notifications etc).

After the user is satisfied with the General settings, they are then directed to navigate to the Ports TAB.

By Right Clicking on the interface, users will be given the Ports menu dialog where they can add or remove ports to listen to. - Select "Add Port" and input a "non standard Remote Administrative Port"

- This implies a port not typical to the base configuration of your controller, in IM3 this port is 9003.

So use of a port OTHER THAN 9003 is recommended.

After users successfully select a port, they then click the "Start Listening" in the lower right of the interface to actively listen on the desired port.

IMPORTANT NOTE: Users must be actively listening to the desired port, before they can successfully test port forwarding configurations.

Step 3: Binary Configuration and Build

Spoiler ([Click to View](#)) After successful configuration of the controller. Users now need the Binary to deploy to HOST machines.

Users must navigate to the "Client Builder" tab in the IM3 Controllers interface.

Network Settings:

IP/DNS: This is the Controllers host address. This is required to be valid and resolvable. Failure will result in the deployed binaries failing to connect for commands from the controller. It is recommended users define a DNS server in place of a physical hard coded IP#. This is helpful for when the controller is either mobile or must deploy the controller software to another system or service. Allowing them to remain in control of the remote administrative machines.

Port: This is the communications port in which all network communication will take place on between the Binary and the Controller. This port must be IDENTICAL to the one(s) configured in the controllers interface (Step2, Ports TAB)

Client Group: This option is used for Client organization and "grouping" Workstation Class

Server Class

Home User Class

etc...

Mutex: This function is similar to a crypters binary string. This is used for the compile portion where this is the encoded "decryption string" allowing the base code to be obfuscated from prying eyes.

- Hit this option only ONCE. (Hitting it numerous times makes no difference, it generates a randomized string) However, always ensure to hit this button on all builds.

Client Startup:

The options and features within this drop down tab are the clients configurations to ensure the Remote Admin service starts up when the machine is booted up, or rebooted.

Unless there are specific environmental conditions to consider, users are best to enable all options within this panel.

Module Protection:

In this portion the builder handles its own binaries protection within the HOST client systems. These options are designed to prevent over zealous security software from removal of the Remote Administrative client assuming it is malicious. Again, unless specific environmental conditions must be met, users are best recommended to enable all options.

Assembly Information and Builder:

These next 2 tabs are pretty straight forward.

Assembly Information: Is the information the binary file will display if the element is inspected by the system. IE - User right clicks and selects the files properties. - This feature is helpful when attempting to camouflage the binary process in with other known windows services or files.

Compile Settings: Straight forward options to compile the client binary.

- Hidden mode will install the service in the systems background, suppressing any dialog boxes. This is also known as "Silent installation"

-- Users must agree to IM3 ToS before Builder will compile any Client Binary.

R.A.T. 101 1.4 v1

Armada - September 18, 2015, 11:30 pm

Written By: [A?mªDa](#)

[Main Course Thread](#)

Introduction to R.A.T. Health and Safety

Spoiler ([Click to View](#))

When we discuss R.A.T. safety and security, we are actually taking on the discussion of 2 very different and unique variables. The Remote Administrative Controllers aspect and The Binary Clients considerations.

It is critical to understand the key differences between the machines being discussed, as some security considerations might be ideal for one but counteractive if applied to the other. It is in this discussion we must now apply the considerations from Section 1.

For our purposes we must assume the following: The Client Binary and R.A.T. Controller must speak to one another in some fashion for successful communication.

The Client Binary is likely to be in "Hostile Wild Environments"

The Remote Administrative Controller must utilize some fashion of layered protection to keep its true location secretive.

Understanding the Hostile Wild

The Internet is a vast expanse of networks of various types of configurations security policies, foot holds, traps and honey pots. It is by these concerns where we treat the Open Internet as a "Wild environment".

It is important to always treat the environment this way when making decisions and determining the considerations required when employing any safety and security strategy.

The primary rule of thumb is almost a paranoia mind set:

"Trust No One, Assume It Can & Will Be Malicious, Take No Unnecessary Risks"

R.A.T. Health

Spoiler ([Click to View](#))

When discussing R.A.T. Health, we are for all intensive purposes speaking about our Binary Client. This is the portion of the Remote Administrative configuration which will be subject to the most scrutiny, have the most liability for security and network related risks. In this section we will examine the A-typical risks associated to Binary installations, the security precautions taken to remove such binaries and counter measures to keep the Binaries healthy and connected to the controller.

R.A.T. Safety

Spoiler ([Click to View](#))

When discussing R.A.T. Security, although there is considerations for both the Remote Administrative Controller and the Binary Client. The Primary focus in this aspect take place on the Controllers side of the equation. This is where the application of the core security considerations and precautions will need to take place, and will ultimately determine the Remote Administrators final success when utilizing R.A.T.s

As we continue in to this discussion it should become very apparent there is a face off and a constant battle when discussing Remote Administrative Technologies.

Through the next section we will discuss in detail every aspect for Health and Safety for both Controller and Client ends of the communication.

R.A.T. 101 2.1 v1

Armada - September 18, 2015, 11:30 pm

Written By: [A?m^aDa](#)

[Main Course Thread](#)

Remote Administrative Controller Security Fundamentals

Spoiler ([Click to View](#))

When we analyze and determine our core security considerations we place focus on the Controlling End. Almost entirely.

In this the Remote Administrator must determine the method of deployment and where the controlling software will reside. Will the controller be deployed to a residential network?

- Example: Remote Admin installs and deploys the controlling software on a LAN based machine they have direct physical access to.

Will the controller be deployed to a remote or server platform?

- Example: The Remote Administrator elects to utilize a virtual or dedicated server service within the internet to be the designated controller. This is useful for topologies which require consistent and constant communication between the controller and the binary client.

How will connectivity between the Remote Administrator be established with the controlling software?

- Example: If the Remote Administrator elects to utilize a remote service or server, how will they establish connectivity to the controlling server, and what protocol will be utilized?

To best make these determinations. We examine the lessons learned from [Section 1.2](#)

The determination of which R.A.T. or Bot will best determine the deployment method. Typical RATs (Such as Luminosity Link, Imminent Monitor, NanoCore) can be deployed to either local or remote locations with relative ease and flexibility.

PHP\Web Based and IRC Based Deployments have more specific requirements, and in general are more suited for remote deployment of the controller software.

Principal Considerations: Controlling Machine should always be kept updated with the latest security updates for all installed software, operating system, and security software.

Any All ports used for services should be configured to "uncommonly used" ports. Unless for explicit rare circumstances, typical communication ports (such as 21, 80, 443, etc) should be avoided to deter network communication conflicts.

Anti viral, Anti-Malware and Firewall policies should be strictly enforced on all controlling machines/servers.

Never give others access or indication where controlling machines or servers are located or accessed. - Unless explicitly trusted.

Controller Deployment to Residential LAN Configuration

Spoiler [\(Click to View\)](#)

In this portion we will examine the typical Home Residential, the Deployment and the Security policies required for successful Remote Administration.

Now, in this diagram it should become apparent there are numerous layers and levels of protection that reside within even the simplest of Home or Residential configurations. Although these configurations are the A-typical deployment for New Remote Administrators, to Expert level. These what are seemingly the simplest and straight forward implementations where the largest problems are encountered.

Typical Security Boundaries & Limitations That Exist In Residential Networks: Internet Service Provider Restrictions

Cable Modem Restrictions or Firewall Policies

Router Firewall and Port Blocking Policies

Computer Security and Firewall Policies

Typical Security Risks That Exist When Utilizing Residential Networks: Remote Administrators
Core\True IP# Being Revealed
Targeted Attacks Being Focused on Remote Administrators Connection
Exploitation of the Controlling Software

Deployment to Residential Network

Prerequisites:

Create a network mapping of every device which connects the end controlling machine, Make a note of every device make and model, verify its security configuration and default settings. (Modem, Router, etc)

Contact or verify that your planned Internet Service provider does not automatically "stealth" or block ports by default. Some unfortunately do.

On the designated controller system, create a list of all security policies, security software, firewall software and Anti viral or Internet Security suites. - This information will become critical for final configuration and deployment of a "Hardened" remote administrative environment.

Deployment:

DISABLE All Anti Viral \ Anti-Malware and Firewall Software. This includes all Operating System defensive measures as well. (Windows Defender and Windows Firewall)

[Install and Configure](#) Your [Chosen R.A.T.](#)

Utilizing the information gathered from your Prerequisite setup, in specific the networking device make and model information, [Port Forward the chosen remote administrative listening port.](#)

Perform Port Testing Using: <http://www.canyouseeme.org> to verify the port is actively unblocked, and accepting connections. NOTE: R.A.T. Controller must be actively listening on the designated port before testing to be successful.

Using Controller Software build 2x Binary Clients - 1x Using the local system loop back hostname of: 127.0.0.1, 1x Using the Real Internet IP# (<http://www.whatismyip.com>).

Using either a Virtualized Machine or Sandboxie Execute the Binary Builds (local loop back first, uninstall, then real host binary) to test connectivity and ensure proper network communication.

- If Local loop back 127.0.0.1 works correctly but real host fails, a networking configuration problem exists and requires further troubleshooting before Administrator should proceed.

Add Exceptions to all Anti Virus and Anti-Malware software for both Controller Binary and a Binary working directory. - For Binary Builds.

[-Allowing your RAT through Windows Firewall](#)

Enable Security software and firewalls.

Repeat steps #4-5 in deployment for port testing and binary connectivity.

At this point you should have successfully installed, configured and secured the Residential deployment of your Remote Administrative Controller.

Secure R.A.T. Residential Routing

Spoiler [\(Click to View\)](#)

When we consider Secure Residential Routing there is 2 avenues to Security.

Firstly, we will discuss why configuration of your Binary clients and use of your Direct IP# is never advisable.

With Remote Administration, it is assumed that the Administrator wishes to utilize stealth and anonymity when utilizing R.A.T. Technologies. If the Home address is utilized the connectivity is easily traced back to the controller.

Secure Routing Example #1 - Best Recommended

Dynamic DNS Enabled Host Address Pointed to a Port Forwarded VPN Network which the controller utilizes for anonymity.

In this example the Remote Administrator has utilized a Virtual Private Network to conceal the true IP# and host address of the R.A.T. Controller. (Including Their Residential and Home address in the process)

This reduces the amount of DNS updates required as the VPN tunnel effectively creates an encrypted data stream between the Binary Clients and the R.A.T. Controller. Including the fact VPN servers are generally statically assigned servers.

Secure Routing Example #2 - LEAST Recommended

Dynamic Enabled DNS Service utilized to point directly to R.A.T. Controllers host address when in use and "Null Pointed" when not in use.

In this example, and the Least Recommended example of Secured Routing for Residential Connectivity. The Remote Administrator utilizes a Dynamic enabled DNS service to point the DNS host address to their IP# when they wish to utilize the Binary clients, and then point to a null IP# address when not utilizing. (Remote Administrator points Dynamic DNS to IP# 127.0.0.1 when not utilizing Controller.)

Why is Example #2 least recommended?

In example #2 we are still directly exposing the Binary Client to the Controllers direct IP#, however we limit the connectivity by null routing when Client connectivity is not required. This can further assist in deterring further analytic of the Binary as it will appear moot in functionality when not in use.

Controller Deployment to Remote Services

Spoiler [\(Click to View\)](#)

In the deployment to remote services, the process is surprisingly simplified, compared to Residential configurations.

In this example we examine the A-typical configuration of a remotely deployed R.A.T. Controller. The deployment of these configurations vary greatly and is best to determine and create a configuration plan based around the servers specifications and the desired binary to be used. (Some remotely deployed solutions require no controlling software, simply services. Example, IRC Binary Clients)

Deployment:

UPDATE All System and Security Software.

DISABLE All System and Security Software.

[Install and Configure](#) Your [Chosen R.A.T.](#) - (If Any)

Perform Port Testing Using: <http://www.canyouseeme.org> to verify the port is actively unblocked,

and accepting connections. NOTE: R.A.T. Controller must be actively listening on the designated port before testing to be successful.

Using Controller Software build 2x Binary Clients - 1x Using the local system loop back hostname of: 127.0.0.1, 1x Using the Real Internet IP# (<http://www.whatismyip.com>).

Using either a Virtualized Machine or Sandboxed Execute the Binary Builds (local loop back first, uninstall, then real host binary) to test connectivity and ensure proper network communication.

- If Local loop back 127.0.0.1 works correctly but real host fails, a networking configuration problem exists and requires further troubleshooting before Administrator should proceed.

Add Exceptions to all Anti Virus and Anti-Malware software for both Controller Binary and a Binary working directory. - For Binary Builds.

Enable Security software and firewalls.

Retest Port's (Step #4)

Controller Security Conclusion

Spoiler ([Click to View](#))

It is my sincere hope, that by the end of this section the reader now has a firm grasp and understanding of the principals to Security, Secure Routing and Deployment of R.A.T. Controller software and Remote service configuration and connection.

In this it is important to always keep security as a top priority as a Remote Administrator. Remember the fundamentals.

"Trust No One, Tell No One, When In Doubt, Don't Do It"

R.A.T. 101 2.2 v1

Armada - September 18, 2015, 11:32 pm

Written By: [A?m^aDa](#)

[Main Course Thread](#)

Introduction to Client Security

Spoiler ([Click to View](#))

My poor pets.

Why do you suffer so? Why are you the little critters whom everyone hates, I love you so dearly. You are the most obvious of solution to a Hacker, yet simply identified, and removed. Purged from existence, if not correctly secured.

The identification of our binary is our true RAT poison.

- Anti virals, Anti-malware, System security policy. all adds up to a lethal dose of a lost Binary. In this section we are going to discuss the preventive measures which must be taken to ensure stability, concealment and above all longevity to our Remote Administrative Binary.

To properly address such security concerns we must clearly understand the levels and measures involved.

Client Security Layers Binary Acceptance and Execution

Spoiler ([Click to View](#))

In this portion it is discussed as 2 possible scenarios for Acceptance and Execution to occur:

- The end controlling machine user downloads or otherwise accepts the binary installation file to the machine and manually executes it.

(User is sent the binary and executes it either knowingly or unknowingly.)

- The binary installation file is "pushed" to the machine and executed.

(Machine is sent the binary file and told to execute via remote script or user to execute on the machine) - Typical to botnet install shops, or transfer of botnets between controllers.

Further notation, this classification also includes web deliverable exploits, 0day exploits or other scripted "download and drop" scenarios.

Binary System Installation

Spoiler ([Click to View](#))

When the Binary file is executed on the client system the binary goes through a series of "steps" to extract the binary data from the crypted file, drop it on the system, place it where it needs to go in the system and then successfully RUN the application instance.

This being said there are numerous areas where the install process will fail.

The most likely reasons a Binary might be accepted and Executed but never installs:Windows System Security Stopped the file (Smart screen, windows defender, windows firewall)

Anti viral software or network appliance detected it the binary

Anti malware or other system security flagged or detected the binary as a potential threat.

The system itself is incompatible. (Sending a x64 bit binary to a x32 bit client for example)

System or Network security policy will not allow execution or installation of software

User account restrictions

Users best counter measures to avoiding a failed install is to use a stable Remote Administrative binary that requires no dependencies. Encode the binary to require Administrative rights to install, and utilize "intelligent" disabling of security precautions.

IE - Many Binary builders or crypters offer "Disable Task Manager" or "Disable Anti virus" etc. use of these features can be very effective in installation, however improper or careless use (ie - checking everything off) will cause the end machine to suspect a problem and likely investigate.

Binary System Integration

Spoiler ([Click to View](#))

It is at this point the Binary will attempt to "Hook itself" to the system. This is where the advertised Rootkits or System integration.

This is ALSO the most likely chance for your binary to be detected and removed. Although system integration is a vital part of the Binary install process, it poses the largest risk because in this step\process the binary will now attempt to merge or place itself or load calls in to the systems core run files.

Example: The system shell, the login service, the browser, etc...

HOWEVER

It is these actions that are going to likely flag the binary as malicious. All system security software runs what is known as a Heuristic engine (Also coupled with the Real time scanner) This Heuristic Engine constantly monitors and scans critical portions of the operating environment looking for unauthorized or unwanted file modifications (Exactly what our Binary will be attempting to do likely)

As little as there is that can really be done about this (Other than disabling of security software). It is BEST RECOMMENDED: to utilize the binary startup options with care, caution, and above all knowledge of what each function will do on the system and why it could potentially flag the binary as malicious.

Heuristic Engine Definition:

A Heuristics engine is part of most if not all security software now a days.

It is for explanation sake a "Database of known system actions or sequences which could potentially be malicious or unwanted"

- It is in essence the "Generic definition file" for viral or malicious code.

Even though it may not know exactly what the file is, it knows what it is doing is likely unwanted or un-welcomed and will likely block the action outright, or prompt the user to confirm\exclude.

System O/S Security Measures\Counter Measures

Spoiler ([Click to View](#))

When speaking about the System O\S Security measures, in general we are speaking of Region Protection, Windows Smart Screen, Windows Defender, and of course Windows Firewall.

It is in these considerations, where we discuss the problems associated to our Binary environments system taking preventative measures. Use of crypters can remove the Region warning (Trusted files vs Files downloaded from the internet) This is typically known as the security prompt as to whether you want to run the binary file obtained from the Internet.

Windows SmartScreen is a fairly new security implementation

However, has proven to be a very effective tool in prevention of Binary malware, or untrusted files. However, as per Windows 7 and above they are the default settings on Windows install, which most users do not modify.

The official method to disable SmartScreen as per Microsoft is straight forward, however not recommended controller side.

Code Open Internet Explorer by clicking the Start button Picture of the Start button. In the search box, type Internet Explorer, and then, in the list of results, click Internet Explorer.

Click the Safety button, point to SmartScreen Filter, and then select Turn Off SmartScreen Filter.

In the Microsoft SmartScreen Filter dialog box, click OK.

Currently, there is no known method to disable Smart Screen from Binary execution, as it prevents the binary from processing before hand.

Windows Defender is another Operating system security measure which has proven to be effective for the more known malware binaries out there. However is relatively ineffective unless the controller is using a very well known binary build such as an old IRC bot, etc.

Windows Firewall, although one of the first of the O\S Security implementations acts as a final guardian to the system before 3rd party external security software comes in to play. It however is the least effective as in its early implementations its constant prompting caused so much user trouble users started blindly accepting the requests, this pattern still exists heavily to this day.

Many crypters and builders can now easily bypass and add rules to the windows firewall without any error or issue.

Software Security Measures\Counter Measures

Spoiler ([Click to View](#))

Software security measures are all things Anti viral, Anti malware and software based firewall\Internet security suites. Although readily disabled by some of our simplest crypters and Remote administrative binary builders, one of the highest debatable areas as to whether it is advisable to actually disable such security measures.

The advantages of disabling such instruments is pretty obvious, no risk of the binary being removed.

HOWEVER the inherited risk associated with such actions is also very straight forward. Most if not all users have become accustomed to listening to their security softwares notifications. Especially when they are told the software has been disabled or corrupted.

This being said, it is MY recommendation to users to not utilize the Disable AV\Anti-malware features, and instead play the Binary Update Game. (Although more work, less likely to raise suspicion)

However, all this being said, is ultimately left to the end controllers decision.

Real time Scanning and Heuristics

Spoiler ([Click to View](#))

Real time scanning and Heuristic Definition Engine are HANDS DOWN the most likely elements to detect, flag and remove a binary install.

But why?

As noted earlier.

Heuristic Engine Definition:

A Heuristics engine is part of most if not all security software now a days.

It is for explanation sake a "Database of known system actions or sequences which could potentially be malicious or unwanted"

- It is in essence the "Generic definition file" for viral or malicious code.

This is coupled, married if you will with the element that the real time scan engine runs the Heuristics definitions. And the real time scan runs at all times, unless of course, disabled.

Real time scan is a major threat to RAT operations as even if the binary is completely undetectable by core standard AV definitions, the Heuristics know to look for other elements other than just the binary code elements which traditional AV definitions are composed of. It instead looks for "actions".

Examples of questionable system actions include:"Silent" or backgrounded download and execute commands

Registry queries

Constant file searching, especially in protected system zones

system file modifications

TCP\IP communications or large piped data requests through an application

Heavy use of system resources (Crypto mining for example)

Although there is no magical solution to avoid these methods of detection given the fact every security software design and their engines vary in functionality, the best recommended practices are: Avoid system file or registry manipulation unless absolutely required.

No heavy uses of system resources

Do not tamper with the Security software itself

Minimize questionable network communications such as large file requests or torrent seeding

Binary Best Practices:

Spoiler ([Click to View](#))

Update your binary, and update often

Utilize a date format in client naming to conform to update standards and verify delinquent clients

Avoid manipulation of client system or protected files unless necessary

Disabling of security software or measures is discouraged

It is at this point I believe the "Golden Rules" need be stated: Do not run a botnet unless required. RATting is not a "fun game" it carries serious penalties if the technology is misused

Your Binaries can and WILL end up in the wild of the internet and will be subject to many various scans and be scrutinized harshly, never assume you do not need to encrypt, or utilize ALL measures of security layering available to you. - Failure to do so will win you a free pair of steel bracelets.

Always assume someone is watching your every action. Someone probably is.

R.A.T. 101 VERSION # v1

Armada - September 18, 2015, 11:40 pm

Final post hold. Reserved for FAQ or other official design.

DaFreak - September 19, 2015, 4:19 am

Amazing tutorial Armada and I loved the way you explained it. Keep up the great work! This should be stickied.

Yakz - September 19, 2015, 4:19 am

I'm literally amazed, as always when seeing the work you put into these contributions, great work Armada!

Mcbride - September 19, 2015, 4:55 am

Armada's dedication to what he does is simply amazing. I dunno how he does it but he does help alot of members here, outstanding work Armada, I appreciate your efforts.

Incendiary. - September 20, 2015, 10:47 pm

Amazing thread, more people need to read this!

Ill be linking a fair few people to this. HQ as always :")

TRAUMA - September 20, 2015, 10:49 pm

Please PM me, I'd love to make this some better graphics xD

Armada - September 20, 2015, 11:19 pm

(Sep 20, 2015 10:49 PM)ZiLo Wrote: [CITE](#) Please PM me, I'd love to make this some better

graphics xD

Your PM button is broken I assume? ?

TRAUMA - September 20, 2015, 11:24 pm

(Sep 20, 2015 11:19 PM)A?mªĐa Wrote: [\[CITE\]](#) Your PM button is broken I assume? ?
No, I just feel special getting the PM first.

Puppeteer - September 21, 2015, 3:18 am

Posting so i can read later.

Great.

NoHax - September 23, 2015, 10:33 am

You are and will stay sick, this is a HQ course!

Raymond Reddington - September 28, 2015, 4:17 am

Only if this section was non profitable and this thread would get a sticky.

Crocs - September 28, 2015, 5:48 am

Very good thread mate. Will be useful for beginners like myself! :)

Armada - October 9, 2015, 7:57 am

Throws the AED against this thread.

I am going to try finish the topicals up this long weekend folks. ?

ROFL OMG - October 9, 2015, 12:31 pm

Love this thread. Everyone should take a look if they have not!

Crazy Chicken™ - October 18, 2015, 8:37 am

bookmarking this thread for the feature

Faluster - October 18, 2015, 1:53 pm

Amazing. Thanks for the work. This is the sort of thread that makes HF such a great place.

johnsonsm - October 18, 2015, 4:06 pm

Yet another good contribution to HF community Armada. Keep up the great work that you do here.
HQ

Brother Mouzone - October 19, 2015, 8:11 am

This thread is amazing.

I do believe we have the makings of the definitive HF RAT 'Bible'.

dnntee - October 19, 2015, 9:12 am

You are and will stay sick, this is a HQ course!

vietcuong91hp - November 4, 2015, 3:02 am

This thread is amazing. thanks in advance !!

Chainfire92 - December 9, 2015, 12:31 pm

great thread, hope it continues :)

RedMarlboro - January 3, 2016, 3:04 am

Awesome guide! Thanks a lot! :) Bookmarked!

supreme00 - January 3, 2016, 3:08 am

since when do paid rats have support lmao

azumx - January 3, 2016, 6:13 am

Thanks for the work. THis thread is amazing

iNeed Sleep - January 3, 2016, 6:20 am

Very informative, detailed post. Thank you very much, I've definitely learned a bit from this.

Yacine95 - January 3, 2016, 4:41 pm

Thank you for this post Armada. As a beginner (with a brain "On"), I appreciate it.

Will you talk about self protection ? how does a rat administrator can hide his steps and how it could fail .

Johnmoe - January 7, 2016, 12:35 am

Best R.A.T Tutorial i ever seen.Thanks u very much for this bro.

Iterator - January 7, 2016, 2:27 am

Amazing thread, thanks for your work.

Ezki - January 12, 2016, 8:59 pm

amazing and very detailed, thanks

?Synapse - January 18, 2016, 7:00 pm

Thanks for the great guide. NanoCore thread you linked is dead btw.

mcifuentes - January 19, 2016, 3:54 pm

OMG Huge tutorial. awesome work Thanks:D

xLabx - January 19, 2016, 3:56 pm

Very good thread bro.is amazing.

ze-slade - January 19, 2016, 3:57 pm

This really deserves to be a sticky. Great job armada.

limb3r - January 19, 2016, 4:55 pm

Very good read. Bookmarked.

Armada - January 20, 2016, 4:03 pm

Thread currently in a Published state will be updated to reflect updated technology, RAT software and networking topologies. ?

Thank you everyone for the support on this thread. It is greatly appreciated.

necromanswer - January 20, 2016, 9:25 pm

Appreciate the effort of writing this up, nice work man.

HFZhyonn - January 28, 2016, 8:04 pm

If I were to buy a crypter from HF what is the one you recommend?

Eilif - January 29, 2016, 5:55 am

Amazing.. No words to describe this.. Gonna bookmark and read later thoroughly when I get to home.

Very interesting topic.

Armada - January 29, 2016, 7:33 am

(Jan 20, 2016 10:25 PM)necromanswer Wrote: [\[CITE\]](#) Appreciate the effort of writing this up, nice work man.

(Jan 28, 2016 09:04 PM)HFZhyonn Wrote: [\[CITE\]](#) If I were to buy a crypter from HF what is the one you recommend?

(Jan 29, 2016 06:55 AM)stefeman Wrote: [\[CITE\]](#) Amazing.. No words to describe this.. Gonna bookmark and read later thoroughly when I get to home.

Very interesting topic.

I am glad the effort is appreciated.

As for a crypter, I personally recommend Byte Protector

Kylo ren - January 29, 2016, 11:19 pm

Thank you for this guide, will use it later,

tunucef - January 30, 2016, 12:08 pm

No need can be removed, thanks.

TazerNips - January 30, 2016, 12:12 pm

Thanks so much for this TuT! Will definately continue reading :D

Angel - January 31, 2016, 8:10 am

thank you for sharing your knowledge and nice tutorial ?

Ramsey - January 31, 2016, 8:14 am

Armada you beast. This is amazing. Thank you for all the time you have put into this

King Cin - January 31, 2016, 8:15 am

Brings me back. Thread looks nice.

Olympiakos FC - January 31, 2016, 11:23 am

Omg Armada this is HQ as fuck homie!Excellent job!

Vu47K - February 1, 2016, 3:28 am

Thanks You soooooo Much For Your Hardworking mate

One of the most impressive and informative thread on HF

Tremendous Information & everything included about R.A.T

Banzaitron - February 6, 2016, 3:27 am

Great post. Read it in one night and took lots of notes. Well done, and thanks for the contribution.

Raymond Reddington - February 6, 2016, 3:31 am

This thread should be a sticky or at least should be in the Premium Hacking Tutorials section.

Definitely worthy of a bronze medal.

Armada - February 6, 2016, 5:08 am

(Feb 6, 2016 04:31 AM)Raymond Reddington Wrote: [\[CITE\]](#) This thread should be a sticky or at least should be in the Premium Hacking Tutorials section.

Definitely worthy of a bronze medal.

Stop stalking me posts M8.

I know you miss me as a leader, but it just cant happen, not with Bull as a man. ?

Love you man <3

1x10x1x10x1 - February 6, 2016, 12:49 pm

The dedication to make all this.. holy shit man! Nice tutorial.

gimi - February 7, 2016, 7:14 am

thank you nice one :)

Kanotix - February 8, 2016, 9:22 am

Wow this tops all the graphics I have come across HF. Nice tutorial. Well Explained.

Memerz - February 8, 2016, 5:16 pm

I love this tutorial. It's very helpful and it explains everything you need to know. Thank you Armada for this course.

Ticoma - February 19, 2016, 9:33 am

This is huge, kudos for creating such a long and in depth article :D

Gizzmo123 - February 20, 2016, 9:30 pm

Amazing tutorial man!! keep it up

Armada - February 20, 2016, 10:04 pm

(Feb 8, 2016 10:22 AM)Kanotix Wrote: [\[CITE\]](#) Wow this tops all the graphics I have come across HF. Nice tutorial. Well Explained.

(Feb 8, 2016 06:16 PM)Memerz Wrote: [\[CITE\]](#) I love this tutorial. It's very helpful and it explains everything you need to know. Thank you Armada for this course.

(Feb 19, 2016 10:33 AM)Ticoma Wrote: [\[CITE\]](#) This is huge, kudos for creating such a long and in depth article :D

(Feb 20, 2016 10:30 PM)Gizzmo123 Wrote: [\[CITE\]](#) Amazing tutorial man!! keep it up
Very glad this tutorial is found helpful.

a lot of work went in to its design, and I intent on running an update very soon, so keep posted. ?

Any questions please hit me up, I will attempt to fix for ya.

bybit - February 21, 2016, 7:53 pm

excellent tutorial sir. thank you very much.. God Bless you :)

dafr34k - February 22, 2016, 1:33 am

good stuff, thank you m9 :) :)

alirezakaj - February 22, 2016, 9:31 am

what a Rat can do at all?

Armada - February 22, 2016, 12:01 pm

(Feb 22, 2016 10:31 AM)alirezakaj Wrote: [\[CITE\]](#) what a Rat can do at all?

RATs allow a user remote system control over another computer terminal.

BeakerShell - February 29, 2016, 9:57 pm

Came across this thread randomly, but thought of givin this 101 a try.

Learned alot from the tutorial and guide. Clear and simple.

Good sharing Armada.

Purple Kief - March 1, 2016, 9:10 am

Great tutorial, bumping this to the top again.

Kurapika - March 4, 2016, 10:23 pm

Amazing tutorial dude... Thank you.

Black.Hawk - March 7, 2016, 6:13 pm

Great! thank you so much, just getting into this stuff. Great way to start!

n0m4dm4n - March 7, 2016, 8:07 pm

Amazing tutorial Armada.

Thank you!

Armada - March 8, 2016, 8:18 pm

Hope this is found useful ?

Goods - March 8, 2016, 9:05 pm

Just took the time to look through all of this. Amazing tutorial Armada. Way to help the community.

Selfpwned - March 13, 2016, 2:33 pm

wow. Thank you for this HQ tutorial!

OrWestSide - March 13, 2016, 2:36 pm

Dont know guys.I downloaded a RAT once and it prompted me to disable my antivirus and windows defender.I was getting suspicious so I did not try it.Maybe when and if I get a new PC i'll try it on my current...

G_LO - March 14, 2016, 2:35 am

Really well done tutorial. Thanks for this tutorial!

madara_uchiha - March 15, 2016, 4:58 am

Nice tutorial. Thanks for sharing it!

drogba - March 22, 2016, 12:39 pm

Nice tutorial thanks what's the best crypter? Thanks

CHAOS - March 30, 2016, 11:59 am

Great tutorial man!

Bumping this up!

Bugs Bunny - March 31, 2016, 3:47 pm

great tutorial thank ya so much :D

UrLocalNewbie - April 2, 2016, 3:51 am

In the tutorials i've seen about how to use a specific tool or create a program they assumed the reader knows already the whole network structure , thats why they werent with much benfit to m but u simply explained the whole thing 101 , this really is a noob friendly post and im sure it'll help ALOT of ppl as much as it helpeed me , Bookmarked keep up <3

EDIT: excuse my spelling mistakes im using the phone :v

Hacker Team - April 6, 2016, 1:43 pm

This is amazing and wonderful thread! Many thanks for sharing!

We have one question: It is possible to configure it with AirVPN? It is compatible with all VPN?

Thank you for clarification. God bless you

Russian Hacker - April 6, 2016, 6:37 pm

thanks so much for this thread. i love it. i learned so much.

overman - April 27, 2016, 7:31 am

Recommend at least 3 undetectable rats on Win10, 8 and 7 in 2016, also:

? How you would create a rat file in pdf, jpg format?

? Why .exe is not converting well?

? Besides .exe, what is your favorite method to infect?

? How you would infect a target without download?

People are getting smarter, there is allot education and articles on the internet about online safety, so how you would

try to infect a hacker - people who are educated about RAT infection?

Armada - April 27, 2016, 8:17 am

Remote admin tools change too frequently to maintain recommendations such as that.

Secondly no RAT remains undetected, if it contains malicious code it will lilely get a definition.

PDF exploits vary and are beyond the scope of this article.

You cant infect image files.

Dont understand what you mean about exe conversion, or other methods other than exe?

RAT Binaries (with few exceptions) must rain as a binary file, otherwise they will fail to function.

overman - April 27, 2016, 8:31 am

(Apr 27, 2016 08:17 AM)Armada Wrote: [\[CITE\]](#) Remote admin tools change too frequently to maintain recommendations such as that.

Secondly no RAT remains undetected, if it contains malicious code it will lilely get a definition.

PDF exploits vary and are beyond the scope of this article.

You cant infect image files.

Dont understand what you mean about exe conversion, or other methods other than exe?

RAT Binaries (with few exceptions) must rain as a binary file, otherwise they will fail to function.

Okay, how about DarkComet RAT, what crypter you would use with it?

Armada - April 27, 2016, 8:41 am

(Apr 27, 2016 08:31 AM)overman Wrote: [\[CITE\]](#) Okay, how about DarkComet RAT, what crypter you would use with it?

Dont use Dark Comet.

Has known vulnerabilities and is out of date. I would recommend Babylon in place.

overman - April 27, 2016, 10:51 am

(Apr 27, 2016 08:41 AM)Armada Wrote: [\[CITE\]](#) Dont use Dark Comet.

Has known vulnerabilities and is out of date. I would recommend Babylon in place.

Babylon, what crypter you would use with it?

Armada - April 27, 2016, 11:00 am

(Apr 27, 2016 10:51 AM)overman Wrote: [\[CITE\]](#) Babylon, what crypter you would use with it?
That would be out of scope for this write up, plus. Honestly I dont really use crypters so you would be best to ask someone who uses them often for a more accurate answer.

I do however know Byte Protector is compatible with it however.

Rubixa - May 13, 2016, 3:40 am

I love how you layed this tutorial out and how you explained it, Bumping this up for obvious reasons!

Threebones - May 21, 2016, 3:22 pm

mind pming me? I can't yet and I need help setting up Ratty (mostly issues with portforwarding cancer)

L33tness - May 21, 2016, 9:50 pm

(May 21, 2016 03:22 PM)Threebones Wrote: [\[CITE\]](#) mind pming me? I can't yet and I need help setting up Ratty (mostly issues with portforwarding cancer)

HMU on skype.

And, is this a new thread? I seem to recall an older one... Or maybe im just thinking of this one. But it is a great post regardless! Good work!

ticorwin - June 8, 2016, 6:22 pm

amazing tutorial! great for beginners to learn

Senor Suave - June 9, 2016, 10:26 pm

Nice man, I appreciate it. Imma read this later and nice theme you got going on.

Armada - June 10, 2016, 7:47 pm

I am in the works of updating this thread to be a more master thread.

All main stream RATs will now be covered and itemized.

I will note there is a possibility of the requirement to rebuild this thread entirely.
Will advise on status later.

Anyone who wishes to assist in the setup guide portion especially those with the Award, please PM me to co-ordinate.

10Clickers - June 12, 2016, 2:20 pm

(Jun 10, 2016 07:47 PM)Armada Wrote: [\[CITE\]](#) I am in the works of updating this thread to be a more master thread.

All main stream RATs will now be covered and itemized.

I will note there is a possibility of the requirement to rebuild this thread entirely.
Will advise on status later.

Anyone who wishes to assist in the setup guide portion especially those with the Award, please PM me to co-ordinate.

As someone new to hacking, what would you advise I start with? Straight to ratting? Or should I start smaller

Armada - June 12, 2016, 5:03 pm

(Jun 12, 2016 02:20 PM)10Clickers Wrote: [\[CITE\]](#) As someone new to hacking, what would you advise I start with? Straight to ratting? Or should I start smaller

Start reading tutorials... That is literally the best solution to someone who wishes to "Break into the field" so to speak.

You must first educate before you explore.

10Clickers - June 12, 2016, 9:31 pm

Wow great guide, you put a lot of time into this

9h057 - June 13, 2016, 7:08 am

Armada this is one of the best tutorials I have ever seen. I will definitely show this to all of my friends and co workers, by the way your amazing work is greatly appreciated!

JBerner - June 13, 2016, 4:07 pm

i am looking for Bots, i prefer quick respond if possible thank you

Armada - June 14, 2016, 2:39 am

(Jun 13, 2016 04:07 PM)Pogosmartiros6969 Wrote: [\[CITE\]](#) i am looking for Bots, i prefer quick respond if possible thank you

Wrong thread, wrong section. Go to the botnet section please.

sam786000 - July 23, 2016, 8:09 am

Excellent tutorial, thanks for the great guide

mastrica - January 30, 2017, 4:01 pm

Amazing tutorial Armada and I loved the way you explained it

HackGuruji - January 30, 2017, 9:35 pm

Amazing tutorial Armada and I loved the way you explained it. Keep up the great work!

Haeavia - January 30, 2017, 10:05 pm

Great stuff, really good for new people!

jamesonboris - January 31, 2017, 4:23 pm

armada i told you paid already for the orcus rat,but am asking you were were am i going to receive the download link but your not replying,i dont understand,you gave me a bitcoin address to pay in of wich i did but you never reply me again,is this real

have been asking you were am i going to receive the license informations but you never replied ,is this is real or something

Armada - February 1, 2017, 4:24 am

(Jan 31, 2017 05:23 PM)jamesonboris Wrote: [\[CITE\]](#) armada i told you paid already for the orcus rat,but am asking you were were am i going to receive the download link but your not replying,i dont understand,you gave me a bitcoin address to pay in of wich i did but you never reply me again,is this real

have been asking you were am i going to receive the license informations but you never replied ,is this is real or something

Clean your inbox out, I can not reply to your messages when your messages are full.

woofr - February 4, 2017, 2:28 pm

How to send RAT to an user and make him execute without letting him know hes executing

something .. Is it possible to have this inside an image or something?

Armada - February 4, 2017, 2:50 pm

(Feb 4, 2017 03:28 PM)woofr Wrote: [\[CITE\]](#) How to send RAT to an user and make him execute without letting him know hes executing something .. Is it possible to have this inside an image or something?

Binary extension obfuscation (spoofing) is an option, although slowly a dying sort of trickery. as the OS systems progress in advancement the developers pick up on these tricks and correct them.

To be tricky in installation it is usually the age old mixture of good masking and straight up social engineering, talk the person in to running the file.

Nothing beats straight up social manipulation.

zerocool1245 - February 5, 2017, 1:43 am

Gratulstions bro! Is there a pdf of this?

Armada - February 5, 2017, 4:16 am

(Feb 5, 2017 02:43 AM)zerocool1245 Wrote: [\[CITE\]](#) Gratulstions bro! Is there a pdf of this?

Na never really thought about doing that, also the guide needs a little bit of updating. You could always just print the web page to PDF I suppose to save a copy to your drive though.

BTW, have not seen that nick name in quite some time. lol

Mika9931 - February 6, 2017, 5:39 am

THANKS

This helped me sooo much, I owe you forever

PeacedGameplays - February 7, 2017, 5:54 am

Nice very helpful! keep up the work and see ya soon!

Shoto - July 4, 2017, 5:23 am

Amazing tutorial Armada you are my saviour :)

Cyber Knight - July 4, 2017, 5:26 am

Armada is a great guy. I do not particularly specialise in RATs and MALwares, but I can say this is a great guide.

pepsiideal - July 5, 2017, 8:33 am

I would like the password please trying to get back into it.

oops wrong place :) too many tabs open :(

Armada - July 9, 2017, 3:22 am

(Jul 5, 2017 08:33 AM)pepsiideal Wrote: [\[CITE\]](#) I would like the password please trying to get back into it.

oops wrong place :) too many tabs open :(

Welp, hope it helped either way :)

(Jul 9, 2017 03:20 AM)xx6x Wrote: [\[CITE\]](#) Thank you for the topic...

Not sure if a spam post or not, but being I am replying anyways, hope this helps in reducing in more ignorant treads..... (jusayin)

Cursedflame1990 - September 16, 2017, 8:49 am

really good explanation man, thanks alot.

js2017 - September 22, 2017, 5:37 am

1. Very nicely written tutorial. Thanks fro putting in the effort.
 2. I am looking for purchasing a RAT, could you point towards a reliable entity.
 3. Also pl tell whether a Crypter should be purchased along with the RAT for FUD.
- thanks

Armada - September 22, 2017, 6:10 am

(Sep 22, 2017 05:37 AM)js2017 Wrote: [\[CITE\]](#) 1. Very nicely written tutorial. Thanks fro putting in the effort.

2. I am looking for purchasing a RAT, could you point towards a reliable entity.
 3. Also pl tell whether a Crypter should be purchased along with the RAT for FUD.
- thanks

The top purchasable RATs currently are

Orcus (my signature)

Imminent Monitor (Owned by Shockwave)

and Netwire (offiste rat, but very stable from what I am told)

As for crypters, I make zero recommendations as they are a day by day thing and I dont think crypting is a great idea to start, it fucks the binary up usually one way or another.

- You cant obfuscate all that code and expect everything to work EXACTLY to design specification, right?

js2017 - September 23, 2017, 12:53 am

(Sep 22, 2017 06:10 AM)Armada Wrote: [\[CITE\]](#) The top purchasable RATs currently are

Orcus (my signature)

Imminent Monitor (Owned by Shockwave)

and Netwire (offiste rat, but very stable from what I am told)

As for crypters, I make zero recommendations as they are a day by day thing and I dont think crypting is a great idea to start, it fucks the binary up usually one way or another.

- You cant obfuscate all that code and expect everything to work EXACTLY to design specification, right?

Thanks Armada for the quick reply. Could you send a link from where Imminent and netwire could be bought. I saw a few but not sure if those were genuine ones.

Also could you suggest a place to get hold of Office exploit.

Thanks in advance for the help.

Armada - September 23, 2017, 9:04 am

(Sep 23, 2017 12:53 AM)js2017 Wrote: [\[CITE\]](#) Thanks Armada for the quick reply. Could you send a link from where Imminent and netwire could be bought. I saw a few but not sure if those were genuine ones.

Also could you suggest a place to get hold of Office exploit.

Thanks in advance for the help.

IM is located in Premium Tool Section of the marketplace.

Netwire is located: <https://www.worldwiredlabs.com/>

JumpT - September 24, 2017, 1:48 pm

Really nice tutorial. Documentation is well done and easy to read, thanks.

WPA2 - September 28, 2017, 4:00 am

I suggest you upload your pics to Pinterest it will load faster, anyways thanks babe<3 great course !Keep up the great work!

LastSession - October 3, 2017, 10:29 am

tbh this needs to be a sticky in the RAT section, well written and very thorough Armada

Armada - October 3, 2017, 11:54 am

(Oct 3, 2017 10:29 AM)LastSession Wrote: [\[CITE\]](#) tbh this needs to be a sticky in the RAT section, well written and very thorough Armada

I got to find time to update this. its outdated the current RATs at least, the theory is still solid though....

blackandblue - October 3, 2017, 7:54 pm

Thank you for this great tutorial

amiirsan - November 1, 2017, 7:13 pm

thank you for this free stuff. haha

can you remove the negative rep please!

NetaXD - November 10, 2017, 8:16 pm

Very good tutorial. Would recommend for anyone trying to learn about the subject!

Hopsin - November 16, 2017, 7:20 am

Great topic. Keep up the good work mate! Have a nice day ?

C@rn@g3 - November 16, 2017, 11:54 am

Highly detailed TUT!!!! Thank you so much for going in major depth for this. ?

Match - November 20, 2017, 6:43 am

Very interesting! :) Is there an E-Book version of this? I'd like to read it in a printed version.

Fadex69 - November 20, 2017, 7:01 am

Very very nice tutorial about rat, thanks :))

Einarsson - November 20, 2017, 8:27 am

Many thanks for this.

I have been looking for an explanation of VPS and VPN control methods, your graphic answered my question.

Post worth it alone for that.

Once again many thanks.

kchaxcer - November 20, 2017, 10:27 am

Thanks for sharing, will look into it!

Kelpo123 - December 1, 2017, 9:19 pm

Thanks for sharing, will look into it!

EarthWizard - December 4, 2017, 2:08 pm

This is a amazing tutorial, thank you so much for sharing it with us!

SwissKing - April 10, 2018, 1:44 pm

I don't get it, new on the forum... where is the actual link to that tutorial?

Armada - April 10, 2018, 1:47 pm

(Apr 10, 2018 01:44 PM)SwissKing Wrote: [\[CITE\]](#) I don't get it, new on the forum... where is the actual link to that tutorial?

You brain dead?

Tutorial is the first 8 fucking posts of this thread. Dumb ass.....

... I gotta update this shit one of these days....

ShadowReaperZ - April 13, 2018, 2:38 am

Great tut! very helpful. Thanks

samar0 - May 29, 2018, 11:04 am

great tut dude, i was printing for manual helper.

Armada - May 29, 2018, 11:05 am

(May 29, 2018 11:04 AM)samar0 Wrote: [\[CITE\]](#) great tut dude, i was printing for manual helper. A good consideration.

I might just write up the proper document for this subject matter.

It is my expertise after all. lol ? ?

samar0 - May 29, 2018, 11:17 am

I have an idea to test the high school security system near in my home, there is a computer lab in high school, my question is there any rat that can infect all the computers connected to the LAN?with one infected client can spread all pc on network lan. sorry for noobie question.

UpTheCrust - May 29, 2018, 11:42 am

(May 29, 2018 11:17 AM)samar0 Wrote: [\[CITE\]](#) I have an idea to test the high school security system near in my home, there is a computer lab in high school, my question is there any rat that can infect all the computers connected to the LAN?with one infected client can spread all pc on network lan. sorry for noobie question.

This thread should provide all the info you need

<https://hackforums.net/showthread.php?tid=5840626>

samar0 - May 29, 2018, 11:48 am

okay thank you for the link, i will reading now.

Armada - May 29, 2018, 12:12 pm

(May 29, 2018 11:48 AM)samar0 Wrote: [\[CITE\]](#) okay thank you for the link, i will reading now. Do not purchase or use Orcus for these reasons.

Simple said, I will ban and report you quicker than you can wipe your harddrive once you realized what I actually did.

Orcus is not designed, developed, or in ANY way intended for bull shit like this.

Go use Dark Comet, or QUasar for fuck sakes.

ag43 - May 29, 2018, 12:52 pm

(May 29, 2018 11:17 AM)samar0 Wrote: [\[CITE\]](#) I have an idea to test the high school security system

near in my home, there is a computer lab in high school, my question is there any rat that can infect all the computers connected to the LAN?with one infected client can spread all pc on network lan. sorry for noobie question.before anything I highly suggest you go check @imaloser's thread in the lounge titled "For all the kids that post about hacking their school/teacher"

" Its a very good informational piece with feedback with some of the communities members, take a very good look at the whole thread before you even attempt to do what you are thinking about, and if you are gonna refuse to listen to any warning at least use something like dark comet for this....

Armada - May 29, 2018, 12:53 pm

(May 29, 2018 12:52 PM)ag43 Wrote: [\[CITE\]](#) before anything I highly suggest you go check @imaloser's thread in the lounge titled "For all the kids that post about hacking their school/teacher"
" Its a very good informational piece with feedback with some of the communities members, take a very good look at the whole thread before you even attempt to do what you are thinking about, and if you are gonna refuse to listen to any warning at least use something like dark comet for this....
Vouch for this.

Know what your getting in to before hand.

samar0 - May 29, 2018, 7:28 pm

i just open discussion because my sisters and my wife pc on the school office has been jacked with fucking rat,all pc on LAN network, thats why i asking some question. i am not kid or fucking student in highschool.and why you give me bad rep dude.i'm 34 old age so not kid :)

UpTheCrust - May 29, 2018, 7:37 pm

(May 29, 2018 12:52 PM)ag43 Wrote: [\[CITE\]](#) before anything I highly suggest you go check @imaloser's thread in the lounge titled "For all the kids that post about hacking their school/teacher"
" Its a very good informational piece with feedback with some of the communities members, take a very good look at the whole thread before you even attempt to do what you are thinking about, and if you are gonna refuse to listen to any warning at least use something like dark comet for this....
I feel so loved lol

Sirru5h made a really useful thread that goes over all the negative consequences about hacking your school here <https://hackforums.net/showthread.php?tid=5840626>

Just in case you want another thread you can reference

(May 29, 2018 07:28 PM)samar0 Wrote: [\[CITE\]](#) i just open discussion because my sisters and my wife pc on the school office has been jacked with fucking rat,all pc on LAN network, thats why i asking some question. i am not kid or fucking student in highschool.and why you give me bad rep dude.i'm 34 old age so not kid :)

You said you planned to test the high school's security. That doesnt sound like you were just looking for open discussion.

ag43 - May 29, 2018, 10:14 pm

Not only that @samar0 your grammar, is that of a middle school student. Not only did you cause confusion but It hurt my head reading your sentences. @imaloser glad you feel the love you deserve it :). Also Samar0 I am starting to understand why your previous account was banned.

priceputu - June 1, 2018, 4:08 pm

Great job armada, i bookmarked this thread

LordDragon - August 9, 2018, 6:57 pm

Great tutorial by HQ member I admire so much.

Drknstrmy666 - *September 17, 2018, 8:49 am*

Super informative. I don't know if I'll ever attempt this but it defiantly gave me a better understanding!

EasternGhost - *October 20, 2018, 3:20 pm*

I'm from a country where port forwarding is not supported by its networks. Is there any other way I can use DarkComet or any other RAT successfully?