Remote Access Trojan

Snehal Sawant, Masira Shaikh
MCA, Mumbai University
Mumbai, India
snehalbsawant2990@gmail.com
masirashaikh93@gmail.com

Abstract— **Remote Access Trojan (RAT) allowing a potentially malicious user to remotely control the system. A Remote Access Trojan is remote control software that when installed on a computer it allows a remote computer to take control of it. A Remote Access Trojan (RAT) allows an attacker to remotely control a computing system and typically consists of a server invisibly running and listening to specific TCP/UDP ports on a victim machine as well as a client acting as the interface between the server and the attacker. The most common means of infection is through email attachments. The developer of the virus usually uses various spamming techniques in order to distribute the virus to unsuspecting users. Malware developers use chat software as another method to spread their Trojan horse viruses such as Yahoo Messenger and Skype. Remote Access Trojans (RATs) are malicious pieces of code often embedded in lawful programs through RAT-sanction procedures. They are stealthily planted and help gain access of victim machines, through patches, games, E-mail attachments, or even in legitimate-looking binaries. Once installed, RATs perform their unexpected or even unauthorized operations and use an array of techniques to hide their traces to remain invisible and stay on victim systems for the long haul.**

Keywords— **RAT, Trojan horse, malware.**

I. INTRODUCTION

A. Definition

The definition of a Trojan horse or short form Trojan varies depending on the source. A widely accepted definition is:

A Trojan horse is an apparently useful program containing hidden functions that can exploit the privileges of the user running the program, with a resulting security threat. A Trojan horse does things that the program user did not intend.

Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include: Deleting data, blocking data, Modifying data, Copying data, disrupting the performance of computers or computer networks.

To make the difference between a Trojan and a virus or worm clear, some characteristics have to be pointed out. A Trojan horse does not replicate or distribute itself on its own.

It does need user actions to start; usually this includes running the host program by intention. Over the years many denotations have been created for different kind of Trojans or related variations, like backdoor, rootkit, remote access Trojan (RAT), key logger, dropper to name a few. Most of them do miss a vital part of the above definition of a Trojan horse. The useful feature of the host program is not present, if there is any host program used for the camouflage at all. Nonetheless we can see them as sub categories of Trojan horses, as the basic idea of fulfilling a job hidden from the user is present in all of them.
For the rest of this paper we will concentrate on remote access Trojans.

II. BACKGROUND ON RAT

A. Scurrying RATs

RATs are malicious programs that run invisibly on host PCs and permit an intruder remote access and control. On a basic level, many RATs mimic the functionality of legitimate remote control programs such as Symantec's pc. Anywhere but are designed specifically for stealth installation and operation. Intruders usually hide these Trojan horses in games and other small programs that unsuspecting users then execute on their PCs. Typically, exploited users either download and execute the malicious programs or are tricked into clicking rogue email attachments.

Most RATs come in client and server components. Intruders ultimately launch the server program on a victim's machine by binding the installing component to some other legitimate program. Intruders can use a program called a binder to combine RATs with legitimate executables so that the RATs execute in the background while the legitimate applications run, leaving victims unaware of the scurrilous activities) In many cases, intruders can customize the server program: set IP port numbers; define when the program starts, what it's called, how it hides, and whether it uses encryption; customize logon passwords; and determine when and how the program communicates. After defining the server executable's behavior, the intruder generates the program, and then tricks the host machine's owner into running it.

RATs are generally sent through emails by ‘riding’ what looks like as a trusted file attachment such as a PDF, Excel spreadsheet or Word doc. Once the victim opens the email and clicks on the attachment, they may actually see a useful or trustworthy looking PDF, XLS or DOC open up but at the same time the RAT is being installed. Some less sophisticated RATs will display a fake error message ‘file corrupted’ so you think the attachment didn’t come through completely and didn’t open. Many RATS can disable antivirus and firewall software or create covert channels to bypass them, when sending and receiving information, commands, data and files. RATs can do just about anything you can think of – this is a sampling of what they are capable of:
¬Watch you type and log your keystrokes
¬Watch your webcam and save videos
¬Listen in on your microphone and save audio files
¬Take control of your computer
¬Download, upload and delete files
¬Physically destroy a CPU by over clocking
¬Install additional tools including viruses and worms
¬Edit your Windows registry
¬Use your computer for a denial of service (DoS) attack
¬Steal passwords, credit card numbers, emails and files
¬Wipe your hard drive completely
¬Install boot-sector (very hard to remove) viruses

A well-designed RAT will allow the operator the ability to do anything that they could do with physical access to the machine. RATs can be used to install additional tools so a program to upload or download files can be installed secretly – what a great way to move an entire electronic copy of an upcoming movie onto a peer to peer file sharing network!

III. SUITABLE CONDITIONS FOR ITS SPREAD

A. Client – server architecture and modus operandi

Remote Access Trojans (RATs) are usually designed as client-server components with the aim of providing the attacker with convenient ways of interacting in real-time with the compromised assets. The client part runs on the compromised machine and sends information to the attacker via email or by establishing a direct connection to the server component, which runs on the attacker’s machine. The attacker would be running the RAT server component, which allows him to manage multiple infected machines at the same time. He will be able to see in real-time the machines that are currently available, the services and applications that they are running, the currently logged on users, security configurations, etc. Further on, the attacker can send commands to be executed by the client component on the compromised machines and receives the results in real time, using the RAT as a fully-fledged remote control.

This architecture also has advantages when it comes to spreading the malicious code to other machines on the network, because it gives the attacker control over the entire process. Instead of having code that automatically proliferates and attacks other machines, like a Worm has (detected by antivirus heuristics), the RATs spread at a click of a button or key stroke on the server side. Like that, the attacker chooses the next target and the time of attack, rather than allowing the malicious code to randomly spread whenever possible, or constantly.

An easy way to comply with the journal paper formatting requirements is to use this document as a template and simply type your text into it.

B. Unique Danger

After you remove most malware programs, the damage is done and the worst of the crisis is over. Not so with RATs. Like their virus and worm cousins, RATs can delete and modify files, format hard disks, upload and download files, harass users, and drop off other malware. It is seen that compromised PCs that intruders used to store games and other cracking tools, taking up nearly all the user's available hard disk space. But RATs have two unique features—content capturing and remote control—that make them a higher order of particularly dangerous malware.

First, the ability to capture every screen and keystroke means that intruders can gather users' passwords, directory paths, drive mappings, medical records, bank-account and credit card information, and personal communications. If your PC has a microphone, RATs can capture your conversations. If you have a Webcam, many RATs can turn it on and capture video—a privacy violation. Some RATs include a packet sniffer that captures and analyses every packet that crosses the PC's network card. Whether you can ever trace these problems back to the RAT is debatable.

Second, an unauthorized user's ability to remotely control the host PC is a powerful tool when wielded in the wrong hands. Remote users not only can manipulate PC resources but can pose as the PC's legitimate user and send email on behalf of the user, mischievously modify documents, and use the PC to attack other computers.

C. Stealth

The key differentiator between a Worm and a RAT is stealth. Worms are designed for constant and quick mass proliferation, execution of hardcoded malicious activity, and possibly calling back home. Their strength is in numbers. RATs, on the other hand, are designed for stealthy deployment and their main purpose is to infect critical assets for as long as possible, and allow the attackers to manipulate them. The main attributes of the RATS that grants them stealth are: no virus signature, ability to bind on legitimate processes, mimicking behavior of legitimate remote access applications and no code to automatically infect other assets.

Not having a virus signature avoids detection through antivirus scans that rely on virus signature databases. The ability to bind to legitimate processes and run in the background enables RATs to avoid detection when the victims analyze the list of running processes. Mimicking the behavior of legitimate remote access application, and not having code that automatically and randomly tries to spread, enables RATs to avoid detection by antivirus engines that run heuristic or sandbox analysis that looks for behavior patterns that are unusual.

D. Damage

Another difference between RATs and Worms is the damage they cause. Worms deliver a series of predefined, hardcoded payloads. They will execute the tasks they were designed for, and try to spread. The attacker cannot interact with the compromised machines. On the other hand, RATs open a door into the network, or into a compromised machine. Through the door, attackers can take over the asset, steal data, gain access to other assets in the network, cause performance degradation or deliver other malicious payloads. The RATs enable execution of custom payloads with real time feedback, while keeping everything stealthy and allowing the attacker to be flexible when selecting targets, or the actions to execute. The payloads to execute may be sent from the attacker's server in encrypted format, so that antivirus engines that scan network traffic in real time cannot detect virus signatures.

IV. CASE

A. Reflecting on the Sony Pictures Entertainment Breach

Gary. S. Miliefsky says that 2015 should be called the Year of the Remote Access Trojan (RAT) instead of the Year of the Sheep. It all started in November, 2014, when Sony Pictures Entertainment (SPE) was hacked. Many speculated it was a 'malicious insider' but the facts show it was something very different and something you should expect when you least expect it.

Let's take a quick look at the SPE attack and realize that it's the tip of the iceberg for what's coming our way in 2015. If you don't take actions and head my warnings to get more proactive in protecting your personal privacy and also in your business environment, avoid being phished and infected with RATs, then you might actually be one of the sheep losing your fleece in 2015.

How Sony Pictures Entertainment Was Hacked – Maliciously From the Outside. The story is an 'internal administrative' password was used to take down Sony Pictures Entertainment (SPE). That is a tiny piece of the real story. It's easy to get an admin password, especially when it's stored in a file called "Usernames &Passwords" in clear text on an adjacent system in the same computer network, if you've already deployed a RAT.

The first problem is that so many computers throughout the globe are infected with zero-day (new) malware. In fact, when NTT tested the top antivirus products for a year, in their recent report, they concluded that between 50-70% of the malware made it passed their antivirus scanners. That means that Antivirus is dead.

Just look at this May 4, 2014 Wall Street Journal article, where Symantec's senior vice president for information security, Brian Dye, told the Wall Street Journal that antivirus "is dead." If you can't detect the malware and you're already infected, then what can it do? How about controlling your computer and using it as one of many 'hops' in the chain to obfuscate the source of an attack? If you get infected with one of these Zero-day RATS (Remote Access Trojans), you're not only a victim, you are an accidental accomplice.

Lex Parsimoniae: Here's What Most Likely Happened Understanding the means, the motives and the capabilities of the 'actors' involved, and using Occam's razor - the least assumptions, problem solved:
1) SPE puts out a teaser in June, 2014
2) A Nation state reacts in June, 2014 and asks both The Whitehouse and UN to halt release of the movie "The Interview"
3) No response to their request and threat to pull "The Interview", to them an 'act of war'.
4) Between July, 2014 and October, 2014, a crack team from a large cyber army is charged with Reconnaissance (RECON) on Sony Pictures Entertainment for the deployment of a highly targeted Phishing attack that deploys a RAT.
5) Internal network RECON takes place, files are stolen by being transferred (uploaded) to other RAT victims, not directly to the attacker, in this case most likely a cyber army.
6) File uploads, email and records pilfering along with hard drive wiping tools were most likely controlled by Command and Control (C&C) RAT servers located outside of the US with other computers controlled remotely inside the US.
7) Pilfered files are leaked, threats are made through spoofed IP addresses accessing gmail accounts to make tracing difficult.
8) 9-11 type threats are made to trick Sony and Movie Theatres into blinking. They blinked.
9) US Government and top security forensic

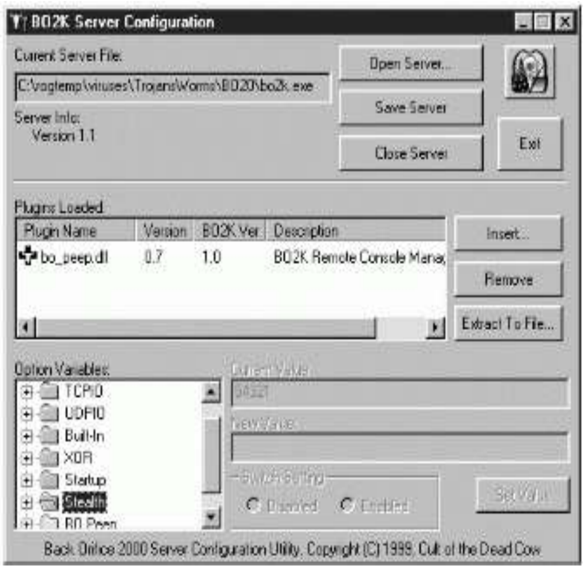
professionals (FBI.gov, Mandiant, Fireeye) figure this all out as well and share some of this information including the fact that the malware was developed on Windows in the Korean language (most likely using WINE running Windows on a Linux derivative OS). The Whitehouse reacts, now that the initial forensics is complete and the POTUS is fully briefed.

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

V. Type of RATs

A. Back Office

The Cult of the Dead Cow created Back Orifice in August 1998. Using the BO2K Server Configuration utility, which Figure 1 shows, an intruder can configure a host of server options, including TCP or UDP, port number, encryption type, stealth activities, passwords, and plug-ins. Back Orifice has an impressive array of features that include keystroke logging; HTTP file browsing, registry editing, audio and video capture, password dumping, TCP/IP port redirection, message sending, remote reboot, remote lockup, packet encryption, and file compression. The program comes with a software development kit (SDK) that extends its functionality through plug-ins. The default bo_peep.dll plugin lets intruders control the remote machine's keyboard and mouse. In practice, the Back Orifice Trojan is unforgiving of mistyped commands; it crashes frequently in the hands of new users but glides unseen in the hands of experienced operators.


BO2K Server Configuration

Current Server File:
C:\vogtemp\viruses\TrojansWorms\BO20\bo2k.exe

Server Info:
Version 1.1

Plugins Loaded

Plugin Name	Version	BO2K Ver	Description
bo_peep.dll	0.7	1.0	BO2K Remote Console Manag

Option Variables:
- TCPIO
- UDPIO
- Built-In
- XOR
- Startup
- Stealth
- BO Peep

Current Value: 54321

New Value:

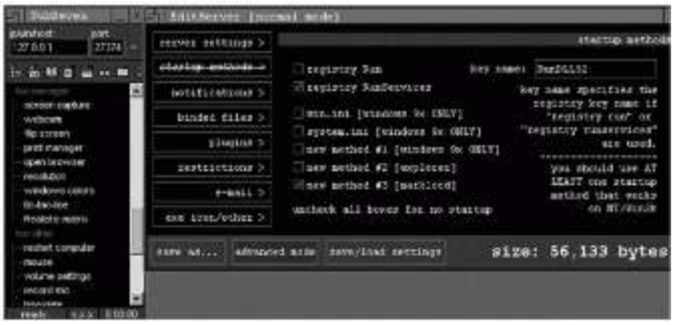
Switch Setting: ○ Disabled ○ Enabled

Back Orifice 2000 Server Configuration Utility, Copyright (C) 1999, Cult of the Dead Cow

Figure 1: Back Orifice interface

B. SubSeven

Even more popular than Back Orifice, the SubSeven RAT is always near the top of antivirus-vendor infection statistics. This Trojan functions as a key logger, packet sniffer, port redirector, registry modifier, and microphone and Webcam-content recorder. Figure 2 shows a few SubSeven client commands and server-configuration choices. SubSeven contains many features to aggravate the exploited user: An intruder can remotely swap mouse buttons; turn the Caps Lock, Num Lock, and Scroll Lock off and on; disable the Ctl+Alt+Del key combination; log off the user; open and close the CD-ROM drive; turn the monitor off and on; invert the display; and shut down or reboot the computer. SubSeven uses ICQ, Internet Relay Chat (IRC), email, and even Common Gateway Interface (CGI) scripting to contact the originating intruder. The program can randomly change its server port and notify the intruder of the change. SubSeven has specific routines that capture AOL Instant Messenger (AIM), ICQ, RAS, and screen-saver passwords.


SubSeven — EditServer [normal mode]

ip/uin/host: 127.0.0.1 port: 27374

startup methods

□ registry Run   key name: [illegible]
☑ registry RunServices
□ win.ini [windows 9x ONLY]
□ system.ini [windows 9x ONLY]
□ new method #1 [windows 9x ONLY]
□ new method #2 [explorer]
☑ new method #3 [notlisted]
uncheck all boxes for no startup

key name specifies the registry key name if "registry run" or "registry runservices" are used.

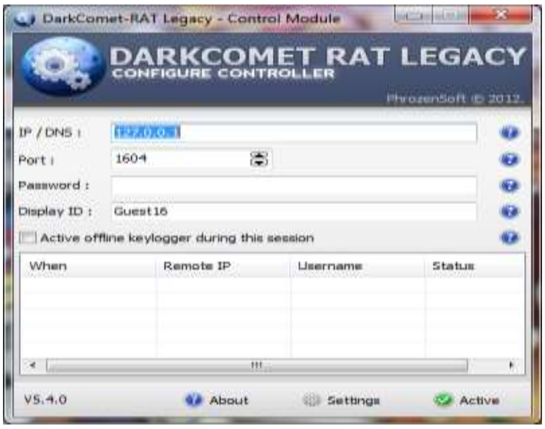
you should use AT LEAST one startup method that works on NT/2k/XP

size: 56,133 bytes

Figure 2: SubSeven client commands and server-configuration choices

C. DarkComet

This was developed by Jean-Pierre Lesueur, an independent programmer and computer security coder from France. Although the RAT was developed back in 2008, it began to proliferate at the start of 2012.DarkComet allows a user to control the system with a Graphical User Interface (GUI). It is commonly used to spy on the victims by taking screen captures, key-logging, or password cracking. In 2014 DarkComet was linked to the Syrian conflict. People in Syria began using secure connections to bypass the government's censorship and the surveillance of the internet. This caused the Syrian Government to resort to using RATs to spy on its civilians. Many believe that this is what caused the arrests of many activist within Syria. Another incident took place in the wake of the January 7, 2015, attack on the Charlie Hebdo magazine in Paris, hackers used the "#JeSuisCharlie" slogan to trick people into downloading DarkComet. DarkComet was disguised as a picture of a newborn baby whose wristband read "Je suis Charlie." Once the picture was downloaded, the users became compromised. Hackers took advantage of the disaster to compromise as many systems as possible. DarkComet was spotted within 24 hours of the attack.



IP / DNS : 127.0.0.1
Port : 1604
Password :
Display ID : Guest16
□ Active offline keylogger during this session

When	Remote IP	Username	Status

Figure 3: DarkComet

D. Moker

This is something new and unbeatable that has hit a red alert in the research world. To date, this APT is unknown and does not appear in VirusTotal". This is Trojan Moker on which even many security agencies have nothing to say except some hypothesis.

Researchers warned that the latest APT to make the rounds features a remote access Trojan that can effectively mitigate security measures on machines and grant the attacker full access to the system.

Moker is an APT – what part of a RAT is not an Advanced Persistent Threat

1. Advanced – Sophisticated techniques undertaken to exploit a system, the sec analysts are unsure what kernel this is aimed at if aimed at any however it can exploit known Windows vulnerabilities and exploit any low level sandboxing MS implemented on their grubs, simply because they can execute boot up code and UAC becomes redundant at software level.
2. Persistent – It's a RAT, how can this "Malware" not persist? contrary to reports, RATs cannot function without a host, the dev will have coded this to constantly relay over intervals, but if a user can create an PPTP, L2TP or SSTP split tunnel to virtually get on the LAN or route over RDP then that agent is always listening and always taking commands. If it had any intelligence it will just salt and hash any dumped data and then encrypt it such as keystrokes and relay over the victims WAN when it's next online, it will decide this on the LAN/WLAN NIC status but again it's pointless unless they are not spearing and specifically targeting orgs.
3. Threat – An entity is required to conduct this attack (Most notably human, but could be your dog) albeit Social Engineering, Phishing, or any other form of network intrusion.

Experts with the Israeli cyber security company enSilo discovered the RAT – which they refer to as Moker – lurking inside one of their customers' networks but admit they aren't sure how it got there. In fact Yotam Gottesman, a senior security researcher with the firm, believes little was known about the malware until they stumbled upon it. Perhaps that's because the RAT, which targets Windows machines, is especially skilled when it comes to not getting caught.

According to researchers, Moker can bypass antivirus, sandboxing, virtual machines, and by exploiting a design flaw, User Account Control, the Windows feature that's supposed to give users a heads up when a program makes a change that requires administrator-level permission. The malware apparently even applies anti-debugging techniques after its been detected to help avoid malware dissection and to further deceive researchers. Moker takes complete control of the target machine by creating a new user account and opening a RDP channel to gain remote control of the victim's device, the researchers explained. It tampers with sensitive system files and modifies system-security settings, and injects itself into different system processes. It's also capable of recording keystrokes, taking screenshots, recording web traffic and exhilarating files. In short, it has a whole gamut of capabilities that come handy to attackers who want to know everything that's happening on a target machine and beyond.

"Interestingly, Moker did not necessarily need to be controlled from remote," the researchers found. "A feature of the RAT includes a control panel that enables the attacker to control the malware locally."This effectively makes Moker also a Local Access Trojan (LAT). "We think this feature was added either for a threat actor to mimic a legitimate user (say, VPNing into the enterprise and then commanding Moker locally), or was inserted by the malware's author for testing purposes yet remained also in the production version," they pointed out.

"Moker's detection-evasion measures included encrypting itself and a two-step installation," Gottesman wrote. Once embedded on a system, the RAT could cause a real headache for users. An attacker could more or less take full control of the device to take screenshots, record web traffic, sniff keystrokes, and exhilarate files. They could also leverage the malware to create new user accounts, modify system security settings, and inject malicious code during runtime on the machine. Ultimately, and unlike most malware, Moker achieves system privileges.

Who's Behind Moker?

A test in our labs revealed that under certain circumstances Moker communicated with a server registered in Montenegro. The Montenegro-based server was referred by several other domains registered in African countries. It’s important to note however that these registered domains cannot give an indication of the threat actor’s identity or physical location as it certainly makes sense to think that the threat actor either used compromised servers or purchased dedicated-only servers in other locations to confuse researchers and law enforcement agencies.

In addition to the measures it takes to avoid detection, another interesting thing about the malware is that it doesn’t necessarily need to communicate with an external command and control server to do its bidding. The malware instead can receive commands locally via a hidden control panel.

The researchers assume the functionality was built into the RAT so an attacker could VPN into the system they’re targeting and pull strings from there, but acknowledge the feature also could’ve been inserted by the author for testing purposes.

While enSilo claims that Moker could have been a onetime thing, the firm wouldn’t rule out the possibility that other RATs might borrow similar techniques later down the line.

“This case might have been a dedicated attack,” Gottesman wrote, “However, we do see that malware authors adopt techniques used by other authors. We won’t be surprised if we see future APTs using similar measures that were used by Moker (such as bypassing security mechanisms and dissection techniques).

Successful attacks against firmware are rare but provide hackers with one thing they covet most: persistence.

Advanced attack groups have already accelerated their capabilities in finding ways to burrow into the BIOS and EFI as noted by the Snowden leaks’ description of the NSA’s attempts to develop malware implants for the BIOS. Further, last year’s disclosure by Kaspersky Lab of the Equation Group’s espionage platform, and specifically a persistence module that targets the firmware of a number of leading hardware vendors, demonstrated how resourced attackers could gain undetectable and perpetual persistence on machines.

These capabilities aren’t limited to nation-state attackers; last summer’s hack of the controversial Italian surveillance software maker Hacking Team also revealed the malware vendor had a UEFI BIOS rootkit at its disposal.

White-hats on the research side have also peered inside the BIOS and UEFI and have begun building tools that help ferret out BIOS root kits.

VirusTotal joined the fray when it announced support for firmware files. Until now, the Google-owned online malware scanner has allowed organizations to upload files and get back a report describing whether leading security tools detect anything suspicious.

A number of sample reports published by VirusTotal list files contained in submitted images and whether they were distributed by the hardware vendor. Such source data is invaluable in determining whether files were inserted by a third party, either along the supply chain or whether the firmware was hacked.

“What’s probably most interesting is the extraction of the UEFI Portable Executables that make up the image, since it is precisely executable code that could potentially be a source of badness,” VirusTotal’s Francisco Santos said. “These executables are extracted and submitted individually to VirusTotal, such that the user can eventually see a report for each one of them and perhaps get a notion of whether there is something fishy in their BIOS image. Additionally, the tool will highlight which of these extracted PEs are Windows targeted, i.e. they will run on the Windows OS itself rather than on the UEFI pseudo-OS.”

VI. CONCLUSION

Typical antivirus scanners are less likely to detect RATs than worms or viruses because of binders and intruder encryption routines. Also, RATs have the potential to cause significantly more damage than a worm or virus can cause. Finding and eradicating RATs should be a systems administrator's top priority.

The best anti-malware weapon is an up-to-date, proven antivirus scanner. Many security administrators rely on Trojan-specific tools to detect and remove RATs, but you can't trust some of these products any more than you trust the Trojans themselves. Agnitum'sTauscan, however, is a top Trojan scanner that has proved its efficiency over the years.

When you suspect that a PC has been infected, disconnect the PC from the Internet so that the remote intruder can't detect the security probe and initiate more damage. Using the Task List, close all running programs that connect to the Internet (e.g., email, Instant Messaging—IM—clients). Close all programs running from the system tray. Don't boot to safe mode because doing so often prevents the Trojan from loading into memory, thus defeating the purpose of the test. Netstat is a common IP-troubleshooting utility that comes with many OSs, including Windows. You can use it to display the entire active and listening IP ports—UDP and TCP—on a local host.

If you don't have a port enumerator to easily show you the culprit, follow these steps: Look for unknown programs in startup areas such as the registry, .ini files, and the Startup folder. Then, boot the PC into safe mode if possible, and run the Netstat command to make sure the RAT isn't already loaded into memory. Then, one by one, execute any suspicious programs you found during your investigations, and rerun the Netstat command between each execution. If a program initiates a connection to the Internet, I give it even more scrutiny. Most Intrusion Detection Systems (IDSs) contain signatures that can detect common Trojan packets within legitimate network traffic. FTP and HTTP datagrams have verifiable structures, as do RAT packets. Properly configured and updated IDS can reliably detect even encrypted Back Orifice and SubSeven traffic.

REFRENCES

[1] 2015: THE YEAR OF THE RAT http://www.snoopwall.com/

[2]Advanced communication techniques of remote access trojan horses on windows operating systems SANS Institute 2004

[3]Operation Shady RAT Mcfee

[4]Remote Administrative Trojan/Tool (RAT) IJCSMC All Rights Reserved

[5] Trend Micro Incorporated Research Paper 2012 Detecting APT Activity with Network Traffic Analysis Nart Villeneuve and James Bennett

[6]www.tusteer.com/glossary/remote-access-trojan-rat

[7]searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan

[8] https://technet.microsoft.com/en-us/library/dd632947.aspx

[9]Advanced communication techniques of remote access trojan horses on Windows operating system

[10] https://en.wikipedia.org/wiki/

[11]http://blog.ensilo.com/moker-a-new-apt-discovered-within-a-sensitive-network

[12]https://threatpost.com/new-moker-rat-bypasses-detection/114948/