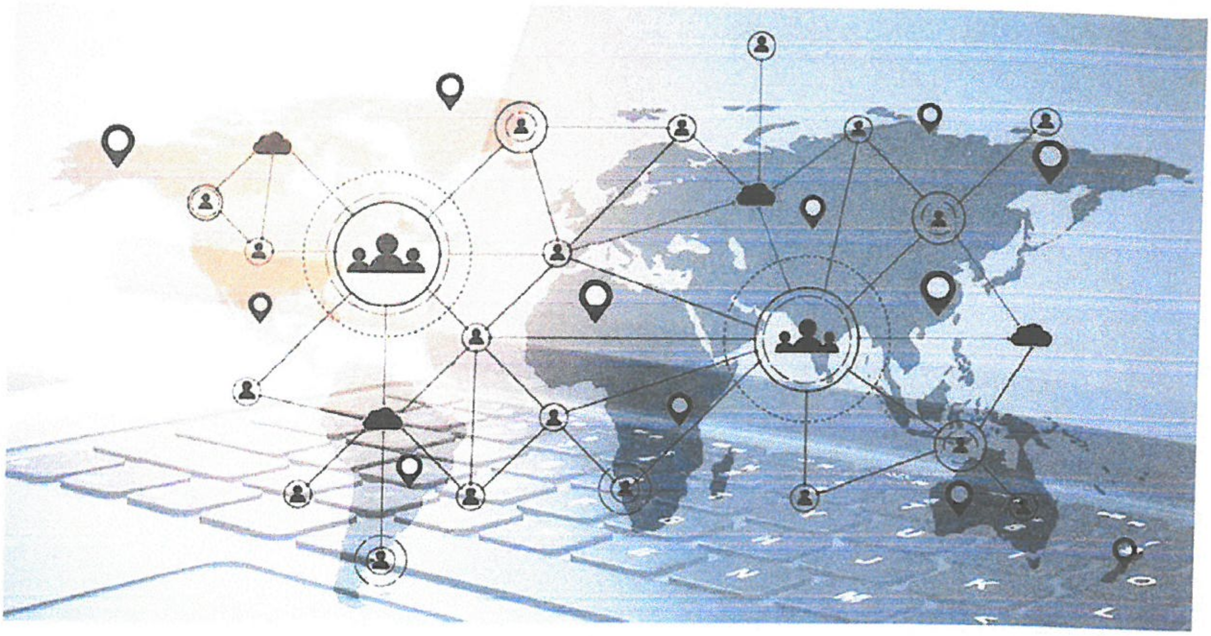
HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-08

REMOTE ACCESS TROJANS



1. Background:

Remote Access Tool is a piece of software used to remotely access or control a computer. This tool can be used legitimately by system administrators for accessing the client computers. Remote Access tools, when used for malicious purposes, are known as **Remote Access Trojans (RATs)**. They can be used by a malicious user to control the system without the knowledge of the victim. Most of the popular RATs are capable of performing key logging, screen and camera capture, file access, code execution, registry management, password sniffing, etc.

2. Remote Access Trojans

RATs, sometimes referred to Remote Administration Trojans are malicious pieces of software that infect the victim's machine to gain administrative access. They are often included in pirated software through patches, as a form of cracked game or E-mail attachments. After the infection, it may perform unauthorized operations and hide their presence in the infected system. An attacker can remotely control the system by gaining the key logs, webcam feeds, audio footage, screen captures, etc.

RATs normally obfuscate their presence by changing the name, size, and often their behavior or encryption methods. By doing this they evade from AV, firewalls, IDS, IPS and security defense systems. Excluding the remote access capabilities, some RATs also behave as a backdoor to the system by infecting it with viruses, worms, spyware, adware, etc. Thus, the infected machines can also be used as a bot or zombie to carry out a chain of attacks to other machines including DDOS.

3. RATs Detection

RATs can be avoided by verifying each piece of software before installation by using authorized program signatures. These program signatures may be available from the vendors of the products; however, it may become difficult to correlate this procedure in an organizational level. In addition, the RATs are using varied level of obfuscation methods to hide their characteristics from detection system. RAT normally injects to legitimate pieces of software or even distributed as patches or other updates, which make them difficult to be captured.

Various host and network-based detection methodologies can be correlated to the proper detection of the RATs. In host-based detection, the unique characteristics of the RATs can be stores in a database level that contains the file name, size, checksum and other unique characteristics. This RATs database can be scanned with the new programs and if matching patterns are found, then can be recognized as RATs. The startup files, registries, auto start and configuration scripts can be monitored and if any distinguished behavior is detected can be detected as a RATs.

In network-based detection method, the network communication protocols can be monitored to check whether if any deviation is there in the behavior of network usage. Ports can be monitored for exceptional behavior, and can analyze protocol headers of packet among the systems. The network traffic can be analyzed and the RAT behavior patterns can distinguish among other legitimate traffic.

4. Examples of RATs

- **Back Orifice**

Back Orifice 2000 (BO2K) was released in July 1999 at DefCon VII, a computer hacker convention held in Las Vegas, Nevada. It was developed by a computer hacker group named "The Cult of the Dead Cow."

BO2K is a client/server application that can remotely controls an information processing application with a fixed IP (Internet Protocol) address by hiding it presence from the victim machine. After its installation, BO2K gathers information, performs system commands, reconfigures machines, and redirects network traffic to unauthorized services.

This RAT should be installed by the end user, and then it will perform its function unknowingly to the user. The B02K installation involves two separate operations, including the client and server. The server part should be an executable one and normally comes in the bo2k.exe name.

B02K has a configuration interface, which can be used to setup the functionality of the program. The configuration interface can be used to setup the Server file, network protocol including TCP or UDP, Port number, encryption mechanism, and password encryption key.

B02K client interface has a list of servers that displays the list of compromised servers and this server has its name, IP address, and connection information. Several commands can be used to gather data from victim machine and this command can be executed using the attacker machine by giving the intended parameters. The responses can be seen using the Server Response window.

- **Bandook RAT**

Bandook RAT has the ability of process injection, API unhooking, bypass the Windows firewall etc. In this, the client has the ability to extend the functionality of the server by sending plugin code to it. The server has capability to hide it by creating a process using the default browser settings.

Bandook has been programmed using a combination of C++ and Delphi. It doesn't uses any cryptographic methods to encrypt, but uses a XORing method. In this, the server part is installed on System32 folder on Windows OS and on its execution; it establishes a connection to attacker, listen for incoming connections on the specified port. Then the attacker can execute the specified server command on the victim's machine. It has spying features like screen manager with screen clicks, cam manager that supports system with multiple cams, live key logger, cache reader, screen recorder etc.

The server component (28,200 bytes) is dropped under Windows, System32 or Program Files, Applications folders, the default name is ali.exe. Once the server component is run, it establishes a connection to the attacking client that listens for incoming connections on a configurable port to allow the attacker to execute arbitrary code from a computer.

- **ProRAT**

ProRAT is a Remote Access Trojan that contains the client and server architecture. It operates by opening a port on the computer that allows attacker to execute several commands on the victim's machine. This RAT has the capability of logging keystrokes, stealing passwords, taking screen shots, view webcam, download and run files etc.

This RAT has features that enable them to undetected from antivirus and firewall; it can run stealthily on the background. It also has the ability to disable and delete system restore points, removing security software, displaying error messages etc.

- **Sub7 RAT**

Sub7 RAT executes on the machine in an undetected and unauthorized manner. Sub7 worked on Windows 9x to Windows XP range OS. Sub7 also has the same architecture of other RAT and allows an attacker to execute server side commands and gain access and information.

One of the distinguished features of Sub7 RAT is that, it has an address book that allows the attacker to whether the victim's computer is online or not.

On the client-side the software had an "address book" that allowed the controller to know when the target computers are online. Additionally the server program could be customized before being delivered by a so-called server editor. A major incident related with Sub7 is that a hacker distributed a mail as that tricked the users to download the RAT and made them compromised.

- **njRAT**

The remote access Trojan is thorough in its data-stealing capabilities. Beyond dropping a key logger, variants are capable of accessing a computer's camera, stealing credentials stored in browsers, opening reverse shells, stealing files, manipulating processes and viewing the user's desktop.

The malware is delivered via spear phishing emails, or drive-by downloads. The attackers are also embedding the malware in other applications such as the L517 Word List Generator; the malware is compressed and obfuscated by a number of tools in order to avoid detection by security software.

Once a victim is infected, the malware is also capable of scanning for other machines on the same network looking for other vulnerable machines to infect. Using that ability to move once inside a network coupled with the legitimate credentials and other data it harvests via its key logging capabilities, njRAT is a classic APT-style attack tool.

The malware stores keystrokes in a .tmp file and connects to a control server over port 1177 registered to an IP address in Gaza City, Palestine. A copy of the malware is stored in a second directory built by the attacker in order for it to execute again upon reboots. Once it connects to the command-and-control server, it sends system information including the computer name, attacker identifier, system location, operating system information, whether the computer contains a built-in camera, and which windows are open.

- **PoisonIvy**

Poison Ivy is a remote access tool that include features common to most Windows-based RATs, including key logging; screen capturing, video capturing, file transfers, system administration, password theft, and traffic relaying.

The Poison Ivy builder kit allows attackers to customize and build their own PIVY server, which is delivered as mobile code to a target that has been compromised, typically using social engineering. Once the server executes on a compromised machine, it connects to a PIVY client installed on the attacker's machine, giving the attacker control of the compromised system.

In 2011, attackers used the RAT to compromise security firm RSA and steal data about its SecureID authentication system. Same year, PIVY also played a key role in the campaign known as Nitro that targeted chemical makers, government agencies, defense contractors, and human rights groups. Just recently, PIVY was the payload of a zero-day exploit in Internet Explorer used in what is known as a "strategic web compromise" attack against visitors to a U.S. government website and a variety of others.

Poison Ivy uses TCP for communication and it is encrypted using Camellia cipher using a 256 key. The key is made from a password created by the attacker while the PIVY server is built.

Many hacker groups used PoisonIvy to attack different category of targets across the world. These include a group called admin@338, which specializes in attacks targeting the financial services industry; th3bug focused on universities and healthcare facilities since 2009. The hacker group menuPass has run cyber-espionage attacks against defense contractors over the last four years

5. Recommendations

The basic requirements for an organization may consist of a decent firewall and an antivirus solution. However, for midsize and large organizations, implementing the tips below can enhance endpoint security, decrease the threat of ransomware or viruses and prevent block threat actors. In the long term, an organization that has successfully established endpoint security, will not be so vulnerable to endpoint attacks.

a. Identify your endpoint

The first step you should take to secure endpoints is cataloging and assessing vulnerabilities. Once you have this data, you can enable network access only to the approved devices and prioritize the most risky and sensitive endpoints. Keep in mind that any endpoint in the network demands protection.

b. Data Access Policy

Many businesses do not have the basic protocols for data storage, access, and usage. Any organization striving to secure its information must outline the data classification levels. For example, data can have a public, restricted or critical access in case of personal or financial information. An organization should define which employees and departments can access each type of data. This can be done with user authentication procedures, such as two-factor authentication. The protocol should notify admins directly of any security breach.

c. IoT Security

IoT devices and printers often have default settings and passwords, which makes them an easy target for attackers. To limit this vulnerability, change passwords regularly release software updates, and maintain the hardware and firmware of all your systems and computers. Windows users, for example, can use automatic deployment rules (ADR) to update or patch their computers.

d. Data Encryption

Encrypt critical and restricted data stored on premises or in the cloud. You can encrypt entire hard drives or specific files, depending on your needs. In addition, to secure data in transit, update all web communication to secure HTTPS protocols. Encrypt emails using Pretty Good Privacy (PGP) or S/Mime encryption. Access remote desktops via Virtual Private Networks (VPN).

e. Enforce Bring Your Own Device (BYOD) Policy

A Bring-Your-Own-Device (BYOD) policy determines the level of support an IT department can provide for computers, smartphones and tablets owned by employees in a corporation. For example, a BYOD policy can include a list of allowed apps and devices in the network, the data they can access, and the websites they can visit. Organization with sensitive information should provide their own laptops or smartphones with restricted and authorized apps and message encryption features.

f. Advanced and Automated Endpoint Protection

Basic solutions for endpoint protection such as antiviruses and firewalls have been in the marketplace for many years. While antiviruses are good in catching known threats using a blacklist, they are struggling to detect sophisticated types of malwares. Firewalls also have their own vulnerabilities. This is why advanced endpoint detection tools use automation to adjust to ever-evolving threats like fileless malware and phishing attacks.

g. Awareness

Make sure everyone in the organization knows how to avoid cyber security threats and risks. Units and offices should include in their TI&E about basic security practices, such as secure password tips and how to identify phishing emails. This type of education should be conducted frequently because of the ever-evolving threats.

6. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://resources.infosecinstitute.com/topic/remote-access-tool/*