2016

An exploration of artefacts of remote desktop applications on Windows

Paresh Kerai
Security Research Institute & School of Science, Edith Cowan University, p.kerai@ecu.edu.au

Vimal Murji Vekariya
Security Research Institute & School of Science, Edith Cowan University, vvekariy@our.ecu.edu.au

DOI: 10.4225/75/58a54f83180cc
Originally published as: Kerai, P. L., & Vekariya, V. M. R. (2016). An exploration of artefacts of remote desktop applications on windows. In Valli, C. (Ed.). (2016). *The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia.* (pp.42-49).

AN EXPLORATION OF ARTEFACTS OF REMOTE DESKTOP APPLICATIONS ON WINDOWS

Paresh Lalji Kerai, Vimal Murji Vekariya
Security Research Institute & School of Science
Edith Cowan University, Perth, Australia
p.kerai@ecu.edu.au, vvekariy@our.ecu.edu.au

Abstract

Remote Desktop Applications (RDA) such as Virtual Network Computing (VNC), Cisco WebEx, GoToMeeting and LogMeIn have been adapted and utilised recently. This is because they facilitate tier-one support to configure computers, networks and solve application-related issues from a remote location. The direct benefit from the use of these applications, is the time (and therefore cost) saving for organisations. Unfortunately, "remoting" technology can also be used by criminals to perform illegal activities, hence remote applications are of key interest to law agencies and forensic investigators. The research outlined in this paper aims to identify any artefacts left behind by common remote applications and technologies used by many firms. These artefacts can be vital to government law enforcement agencies and forensic investigators, as they could be used as evidence in cyber-crime investigations. This research will focus on RealVNC, TightVNC, Cisco WebEx, GoToMeeting and LogMeIn applications. The findings from the research shows some artefacts left behind by the applications, which can be used by forensics investigators or law enforcement for possible evidence.

Keywords
Virtual Network Computing, Computer Forensics, Encryption, Computer Security, Remote Desktop

INTRODUCTION

RDA allow organisations and individuals to access a computer or network remotely, where physical access to the network is not available or where access to the device is impractical. Such applications facilitate access to computers as though a user is sitting right in front of his/her computer. There are various types of RDA currently used by many organisations and individuals such as VNC, LogMeIn, Citrix GoToMyPc, LogMeIn and TeamViewer. The increasing adoption and use RDA has also increased the potential for cyber threats to be realised against organisations

However, using the application can be slow over the internet depending on the Internet connection speeds. Some remote applications such as VNC have had security issues in past due to using weaker encryption implementations (Kerai, 2010). It is plausible that similar issues exist in other remote applications, or still exist in VNC.

In this paper, we detect and retrieve any artefacts left behind by RDA on a Windows computer. Client software for five common remote applications (RealVNC, TightVNC, LogMeIn, Teamviewer and Citrix GoToMyPc) will be installed individually on a Windows 10 computer, and test remote connections will be initiated that we expect will create configuration changes on the computer. The information will be forensically analysed to find any artefacts left by the application on the computer. The paper outlines the location of the artefacts and the types of information left by the application.

RealVNC, TightVNC, LogMeIn, Teamviewer and Citrix GoToMyPc remote applications was used for to conduct the research. The findings will show whether the R leave any artefacts, and this can help law enforcements for forensic investigations.

BACKGROUND

Computer forensics is computer science used to aid legal process in investigations (Brown, 2006). It is the process of obtaining, identifying, extracting, analysing and documenting digital evidence for use as evidence in legal case (Brown, 2006; Kerai, 2010). However, forensics analysis need to be followed in a defined procedure which is accept by the law court. A guideline defined in HB171 (HB171, 2003) is currently used as a guide to carry out forensics investigations and manage electronic evidence.

It is important to follow a standard procedure when performing acquisition of electronic evidence when performing a forensic investigation (Hannay, 2008). It is important to acquire the evidence without modifying or damaging it and validating the evidence is the same as original. This is done by chain of custody and documentation.

Forensic analysis for remote protocols has been an area of interest for the law enforcements and other government and state agencies. This is because these applications can be used to also perform cyber-crimes and illegal communications. A previous research done by (Kerai, 2010), showed that VNC and Microsoft Remote Desktop Protocol left behind artefacts, connection and application logs on a computer system locally. The research showed that the VNC application and Remote Desktop Protocol leaves some artefacts on the Windows Registry File System and other also connection and other application logs on the computer system locally.

REMOTE DESKTOP APPLICATIONS

Demand for RDA has increased with time, where a user can remotely connect, manage and configure another computer or networks. Connectivity between a user's computer to another remote computer can be achieved with readily available hardware and software to connect you virtually to any remote network. The constraint is cost and bandwidth issue that is associated with some technologies (Hoogenboom & Steemers, 2000).

There are various remote desktop applications and technologies available in recent years that can be used to remote in and fix a computer related issues. Online tools like LogMeIn and Citrix GoToMyPc are easy to use, reliable and secure (TeamViewer, 2016). However, standalone applications such as RealVNC, TightVNC, UltraVNC, Teamviewer and others are applications will require the user to configure the application on the computer for a remote connection, which may require some technical skills.

VNC (Virtual Network Computing) - VNC was first developed by the Olivetti and Oracle Laboratory as their telephony system. Later the technology was acquired by AT&T labs and the owners of the technology formed RealVNC to continue working with the remote technology.

The VNC application uses a Remote Frame Buffer protocol to remote access a graphical user interface of the connected device. The application uses TCP 5900 and TCP 5800 for web based remote access. Hence it enables users and organisation to access network resources remotely over the internet. The application has two independent versions, the client and the server, both versions run on most operating system platforms. This makes it very popular as anyone using Windows operating system can remote in to a Linux-based computer or Mac OSX based computer and vice versa. However, a server instance needs to be installed on a computer and a client is then used to access the server. Previous research has shown and discussed the results on how the VNC connection works and the security features and weakness it has (Kerai, 2010).

Other remote support applications such as LogMeIn, GoToMyPc and Teamviewer use TCP port 443 and have different application architecture and implementation than VNC application, due to them being web client based rather than standalone. Hence the artefacts might be different compared to VNC application.

Next session outlines the lab setup and materials used to analyse the remote applications. The research outlines artefacts left by the applications and individual or remote connection information. These artefacts and information can be used by forensics investigators and law agencies in court of law as evidence, in a cyber-crime related criminal case.

EXPERIMENTAL SETUP

Various software and tools were used during the data collection, acquisition and analysis of the raw dd image of the Windows operating systems (see table 1). Different virtual machines and images were used to analyse the application independently.

Table 1: Tools used in Experiments

Applications	
VMware Workstation v12 professional	Windows 10 operating system was installed and created separate instances of each application for analysis.
Remote Desktop Applications	• Real VNC version 5.3.2 • TightVNC version 2.7.10 • Citrix GoToMyPC • Teamviewer • LogMeIn
Password Recovery Tools	• Abel and Cain v 4.9.35 – This is a password recovery and sniffing tool used to capture network traffic and sniff passwords. • VNCPass • VNCSniff
Windows File System Tools	• Microsoft Sysinternal Suite

ANALYSIS

All RDA were independently analysed on a virtual machine running the Windows 10 operating system. An ADSL router by default does not have remote connections to computers externally, this is because the router does not have remote protocol ports open on the router firewall. For VNC connection to work the user needs to open TCP port 5900 and TCP port 5800 for the Java client. However other mentioned remote applications run on TCP port 443, therefore they do not need special ports opened on the router. Once a VNC application is installed on a computer it automatically opens the ports on the local Windows firewall.
VNC applications use Data Encryption Standard (DES)which has proven to be insecure due to its small key size (56-bit). Due the weak encryption algorithm, an attacker can sniff the traffic after cracking the encrypted password.

Windows Registry Analysis

The Windows registry is a central hierarchical database used by the Windows Operating System, to store all the information that is necessary to configure and manage applications and hardware devices installed on the system (MicrosoftSupport, 2016). The registry hive is a group of root keys and sub keys that contain application data (Alghafli, Jones, & Martin, 2010). There are five logical hives in the Windows Registry, the application registry values are most stored under the HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE and HKEY_USERS registry hives.

RealVNC

RealVNC configuration is stored in the Windows registry, including encrypted login passwords, settins and outbound connections made to the RealVNC servers. The default Windows registry viewer was used to analyse the data and artefacts of the application. The connection server password used by the RealVNC server is encrypted with DES encryption, since DES encryption is weak, the password can be retrieved easily. Tools such as Cain and Abel, VNC Crack and online password cracking web services can crack DES encryption with no cost, due to readily available tool to decrypt the encryption. Table 2 shows the artefacts left by RealVNC application on Windows 10 machine.

Table 2: RealVNC Windows Registry Analysis

Under HKEY_CURRENT_USER\SOFTWARE\RealVNC\vncviewer\MRU, the application stores all the history of the external IP addresses connections made to an external VNC server.
Under HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver, the application stores encrypted password of the RealVNC server. The password is encrypted with DES encryption standard. Since DES is a weak encryption standard, decrypting the password is possible.
Under HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver, the application also stores configuration settings such as, if the application is personal or enterprise edition, RSA private key and the authentication scheme used.
Under the HKEY_USERS\Software\RealVNC\vncserver, the application stores the vncserver license key.

Table 3: RealVNC Logs on Windows File System

• The application leaves log information in the Windows Event Viewer under the Application Logs. The logs show client IP address that made the connection to the RealVNC server, and the connection logs for the computer made a connection to another VNC server.
• The RealVNC application stores the connections and application log settings on the hard drive. The log file includes all the connection details, including the client IP address and any files transferred during the connection. The file is located under C:\Program Files\RealVNC\VNC Server\Logs or C:\Program Files (x86) \RealVNC\VNC Server\Logs. However, by default the application logging is not enabled, therefore a user will need to enable logging for the logs to be generated.
• By default, Windows Firewall logs are not enabled, therefore no log information is kept if a VNC connection is made inbound or outbound. However, if the Windows firewall logging is enabled, then the VNC connection is logged on the log file. The firewall log file is located under C:/Windows/System32/LogFiles/Firewall
• The application stores the chat conversation logs under the folder C:\Users\admin\AppData\Local\RealVNC.

TightVNC

TightVNC is a free application, and works the same way as RealVNC. The application also stores the application settings and logging information on both the Windows Registry structure and locally on the computer hard drive. The connection server password used by the TIghtVNC server is encrypted with DES encryption, in a similar way to how RealVNC server encrypts its password. As stated early the encryption is weak and can be defeated easily to retrieve the server password. The table below shows the artefacts left by RealVNC application on Windows 10 machine.

Table 4: TightVNC Windows Registry Analysis

• Under HKEY_CURRENT_USER\SOFTWARE\TightVNC\Server, the application stores the configuration settings for the TightVNC server, this includes also the encrypted password for the server. This password is used to connect to the server. • Just like RealVNC the connection password is encrypted with DES and therefore password can be attacked with password cracking tools.
• Under HKEY_CURRENT_USER\SOFTWARE\TightVNC\Viewer, the application stores all the connection history of the local computer making VNC connections outbound. Therefore, the registry key stores all the IP addresses the TightVNC server has made connection to another external VNC server.
• Under HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC\Server, the application also stores the configuration settings for the TightVNC server, this includes also the encrypted password for the server. This password is used to connect to the server.

Table 5: TightVNC Logs on Windows File System

• The application leaves log information in the Windows Event Viewer under the Application Logs. The logs show client IP address that made the connection to the TightVNC server, and the connection logs for the computer made a connection to another VNC server.
• The application stores the connections and application log settings on the hard drive. The log file includes all the connection details, including the client IP address and any files transferred during the connection. The file is located under C:\ProgramData\TightVNC\ Server\Logs. However, by default the application logging is not enabled, therefore a user will need to enable logging for the logs to be generated. • Also, the application does not log any outgoing VNC connections, therefore if a user makes a VNC connection to an external VNC server, no logging information is kept by the application.
• By default, Windows Firewall logs are not enabled, therefore no log information is kept if a VNC connection is made inbound or outbound. However, if the Windows firewall logging is enabled, then the VNC connection is logged on the log file. The firewall log file is located under C:/Windows/System32/LogFiles/Firewall

Citrix GoToMyPc

Citrix GoToMyPc is an application that can be used to access remote computers over internet connection. Unlike VNC applications, GoToMyPc application does not require client and server, allowing invitations to other users to remotely access their computer. The connection is done over HTTPS 443 TCP port; therefore, it does not require to have an independent port open on the firewall to work.

The user initially will need to register on the Citrix GoToMyPc website and add remote computers to the registered account. However, the remote computers need to have a GoToMyPc installation to receive the remote connections. User will need to log in to the account and then initiate a remote connection by selecting the computer defined on the user account. Someone can also send out an invite to connect a computer that is not registered to the account and initiate a connection if accepted by the guest user. The application uses end to end encryption during the remote connection using the AES 128bit encryption standards (GoToMyPc, 2016). The table below shows the artefacts left by RealVNC application on a Windows 10 machine.

Table 6: GoToMyPc Windows Registry Analysis

• Under HKEY_LOCAL_MACHINE\WOW6432Node\Citrix\GoToMyPc, the application stores all the configuration settings. The settings include encrypted access code with Advanced Encryption Standard (AES) 128-bit encryption standard, email address of the person the account is registered under and other various settings.
• The application also keeps are the records of guest invites send to connect to the GoToMyPc workstation. These settings can be located under HKEY_LOCAL_MACHINE\WOW6432Node\Citrix\GoToMyPc\GuestInvite.
• Under the registry value HKEY_CURRENT_USER\SOFTWARE\Citrix\GoToMyPc\FileTransfer\history and HKEY_USERS\S-1-5-21-97110503-761733263-3747825532-1001\SOFTWARE\Citrix\GoToMyPc\FileTransfer\history, the application stores the hostname of the computer made the remote connection, including the location of any files transferred during the remote session process.

Citrix GoToMyPc application did not log any access or connection logs on the local computer. The application instead stores the connection logs on the user's GoToMyPc online account. Hence no logs were available on the local computer of any type of connections made or received. Also, no connection or applications logs were stored on the Windows Event Viewer logs.

Teamviewer

Teamviewer is an organisation founded in 2005 in Germany that provides web based collaboration solutions and remote desktop capable support to the users. The application can be used by users to remotely control another computer that has the application installed on it. The application works over TCP port 443 and uses RSA public/private key exchange and AES 256-bit session encryption to secure the connection traffic (TeamViewer, 2016). The table below outlines artefacts left behind by the application on the Windows Registry File Structure.

Table 7: Teamviewer Windows Registry Analysis

• Under HKEY_CURRENT_USER\SOFTWARE\Teamviewer; registry key value, it stores the application settings including the account name of the Teamviewer account. This is the email address used to login on to the Teamviewer account. The application also stores the username of the local computer.
• Under HKEY_LOCAL_MACHINE\WOW6432Node\TeamViewer and HKEY_USERS\S-1-5-21-97110503-761733263-3747825532-1001\SOFTWARE\Teamviewer; registry values, the application stores the all the encryption keys and certificates that is generated, when a remote connection is initiated and other Teamviewer settings.

Table 8: Teamviewer Logs on Windows File System

• The application stores the incoming connection logs under the C:\Program Files (x86) \TeamViewer\Connections_incoming, the file includes all the incoming connections to the computer. However, Teamviewer doesnot use an IP address or email address for initiating a remote connection, instead it uses a unique random generate number, which is used as a ID to initiate a connection.
• Under the same folder C:\Program Files (x86) \TeamViewer\, Teamviewer stores a log file named "TeamViewer11_Logile", this file contains all the remote connection information, including the client ID, the public IP address of the client that made the connection, log entries for any files transferred during the remote session. This is crucial for the forensic investigation as it can be used to track down an individual with a Public IP address.

The application stored no connection or applications logs were stored on the Windows Event Viewer logs.

LOGMEIN

LogMeIn provides remote connectivity solutions to organisation for collaboration and IT management. The organisation was found in 2003 and provides servers to user to access and connect to remote computers. The LogMeIn client initially establishes a connection to LogMeIn servers and authenticates itself with a TLS1.X certificate. Once the identity is verified the user can then connect to and exchange data to another host to computer associated to the LogMeIn account. The application uses TLS based certificate authentication and uses AES or Triple Data Encryption Standard (3DES) encryption 128-bit or 256-bit encryption standards (LogMeIn, 2016). The table below outlines artefacts left behind by the application on the Windows Registry File Structure.

Table 9: LogMeIn Windows Registry Analysis

• Under the registry key, HKEY_CURRENT_USER\SOFTWARE\LogMeIn\Toolkit\DesktopSharing, the application stores the last guest recipient email address used to invite a user to remote into the computer.
• Under the registry key, HKEY_CURRENT_USER\SOFTWARE\LogMeIn\Toolkit\Filesharing, the application last guest recipient email address used to share a file transfer from the computer.
• Under the registry key, HKEY_LOCAL_MACHINE\SOFTWARE\LogMeIn, the application stores all the configuration settings and user preferences. The registry value also stores user guest invite settings.
• Under the registry key, HKEY_LOCAL_MACHINE\SOFTWARE\LogMeIn\V5\WebSvc\Shared, the application stores details about any files shared to the remote user.

Table 10: LogMeIn Logs on Windows File System

• LogMeIn application logs all the connection logs both incoming and outgoing to a log files located under the C:\ProgramData\LogMeIn folder. There are two logs files that contain connection settings including the public IP address of the remote user and basic remote connection settings used for the connection. • The log files also contain information about file transfers and send over to remote computer, such as name of the file, location of the file and file type. • The logs also contain details any incoming remote connections initiated to the computer by an external remote user. This includes the public IP address of the computer initiating the remote connection.
• The application incoming and outgoing remote connection is stored and captured on the Windows event viewer, under the Application logs. The log entry stores public IP address of the guest user connecting to the computer. • Once the remote user ends the connection or logged out, another log entry is created capturing the event with the IP address and the time stamp of the connection.

As identified above on the results, the RDA do leave behind useful artefacts such as IP addresses and email addresses of individuals who have remoted in a computer. This information can be used by law agencies and forensic investigators to prosecute or assist them to develop their investigations further. The application incoming and outgoing remote connection is stored and captured on the Windows event viewer, under the Application logs. The log entry stores public IP address of the guest user connecting to the computer. The logs also show information such as file name, type and location of files been transferred to the remote computer. This can be used to find exactly what the kind of files were transferred and the location of the file on the local and remote computer. All the applications store some sort of encrypted credentials and certificates on Windows registry hive. However, VNC applications store server connection password on DES encryption standard, a less secure and can be cracked easily by password cracking tools.

Comparing the results of previous research done by (Kerai, 2010), there is not a much difference on how RDA leave behind artefacts. Especially RealVNC and TightVNC applications do leave behind reasonable number of artefacts including the connection encrypted password used by the applications

CONCLUSION

Remote desktop applications provide end users and organisations the ability to remote in to networks and computers to manage and troubleshooting network related issues. Due to its ease and graphical interface, the adoption of remote access application is rapidly increasing. There are benefits of RDA to organisations and individuals, however the technology can also be exploited by criminals, cyber groups and terrorist groups to perform illegal activities on remote computers and networks.

As shown above, several RDA leave behind local artefacts which can be of importance to forensic investigation. This is a large impact to government law enforcements agencies and forensics investigators to recover any potential artefacts left behind by the applications on the computer for further investigations. The artefacts can be used to investigate crimes committed by individuals who have transferred explicit, illegal and terrorism relates materials and documents over the remote connection.

The research conducted has verified that the remote applications do leave artefacts behind and can be assessed and reviewed in forensically sound manner. Further research will explore and compare other remote applications, along with evaluating the applications use on different operating systems. Providing further important artefacts that can be of a forensic interest.

REFERENCES

Alghafli, K. A., Jones, A., & Martin, T. A. (2010). Forensic Analysis of the Windows 7 Registry*Australian Digital Forensics Conference, held in Perth, Western Australia. Australia,*

Brown, C. L. T. (2006). *Computer Evidence: Collection and Preservation*. Massachusetts: Charles River Media, Inc.

Hannay, P. (2008). *Forensic Acquisition and Analysis of the TomTom One Satellite Navigation Unit*. Proc. xxth Australian Digital Forensics Conference, Perth, Australia.

HB171, S. A. I. (2003). Guidelines for the Management of IT evidence. Sydney: Standards Australia International Ltd.

GoToMyPc, C. (2016). GoToMyPc Technology Security White Paper. Retrieved from https://www.gotomypc.com/downloads/pdf/m/GoToMyPC_Security_White_Paper.pdf

Hoogenboom, M., & Steemers, P. (2000). Security for Remote Access And Mobile Applications. *Computer & Security*, *19*(2), 149-163. Retrieved from http://www.sciencedirect.com.ezproxy.ecu.edu.au/science/article/pii/S0167404800878256

Kerai, P. (2010). *Remote Access Forensics for VNC and RDP on Windows Platform.* Bachelor of Computer Science Honours Edith Cowan University, Perth, Australia.

Kerai, P. (2010). *Remote Access Forensics for VNC and RDP on Windows Platform*. Proceedings of the 8th Australian Digital Forensics Conference, Perth, Australia.

LogMeIn. (2016). LogMeIn Security An In-Depth Look. Retrieved from https://secure.logmein.com/welcome/documentation/EN/pdf/common/LogMeIn_SecurityWhitepaper.pdf

MicrosoftSupport. (2016). Windows Registry Information for Advanced Users. Retrieved

TeamViewer. (2016). TeamViewer Security Information. Retrieved from https://downloadap1.teamviewer.com/docs/en/TeamViewer-Security-Statement-en.pdf