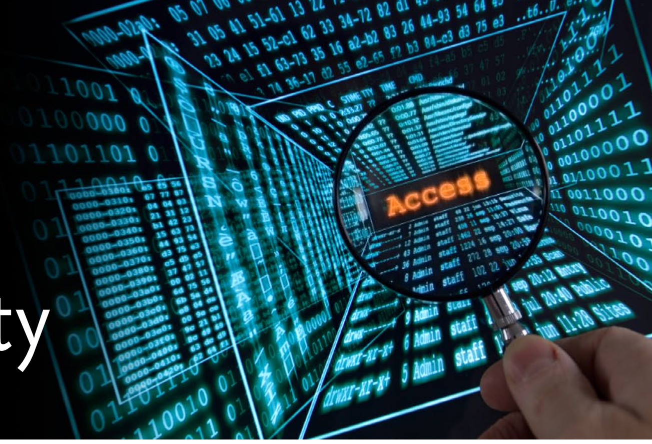

Remote Access Security

How big an issue is it? What can you do?

In March 2013, as reported by ZDNet, Computerworld and other media outlets, a popular and well-known remote access solution was compromised by a group of hackers in a plot to "target activists, industrial, research and diplomatic targets".[1] The attacks installed malware which was designed to take screenshots, gather information about systems and local accounts while also scanning local hard drives for specific file types.

Stories like this are becoming all too common as nearly every week we hear of another organization falling victim to some type of cyber-crime, be it fraud, theft or hacking. In 2012, our connected world of machines, devices, people and networks resulted in more than 900 reports of theft or loss of data with six instances alone resulting in nearly 40 million records being compromised.[2] Despite numerous warnings, extensive media coverage and corporate security policies, companies continue to struggle with cyber threats.

Complicating matters is the sheer number of connections that exist. From smartphones, tablets and laptops to ATM machines, server farms and building sensors, most of today's devices connect to the Internet. When unprotected, each represents an exploitable opportunity for hackers that can lead to significant damages.

For example, using a service like Shodan - a type of search engine for finding devices connected to the Internet – hackers have access to a trove of information about potential security vulnerabilities. They can then use freely available remote access software to help carry out attacks. Remote access software offers invaluable business benefits, but the unfortunate reality is that 88%[3] of all hacking attacks occur via remote access tools.

With the right knowhow, patience and a few Internet searches, hackers can exploit vulnerabilities from virtually anywhere in the world. And as the number of connected devices continues grow so to do the opportunities for cyber-crimes.

> The team behind these recent attacks has been active since 2008, possibly since 2004. They exploited an application commonly used for remote administration - with legitimate digital certificates and more than 100 million users - to target activists, political figures and national information **agencies.**
>
> - KASPERSKY LAB REPORT, VERSION 1.02, MARCH 2013

NOTEWORTHY HACKING INCIDENTS

YEAR	COMPANY	RECORDS IMPACTED
2012	Zappos	24,000,000
2011	Sony Corporation	77,000,000
2011	SK Communications	35,000,000
2009	Heartland Payment Systems	130,000,000
2009	RockYou, Inc.	35,000,000
2007	TJX Companies	94,000,000

Source: DataLossDB - www.datalossdb.org

So how can an organization ensure that it's taking every precaution when using a remote access solution?

The key is deploying a multi-layered approach where security is the foremost concern. Begin by adopting proper training and procedures for staff. For many industries, compliance regulations such as HIPAA and PCI provide frameworks to follow, including specific guidelines covering remote access.

In addition to policies, companies can invest in solutions like Netop Remote Control. Netop has been providing secure remote access for nearly 30 years. Unlike some of the more popular remote access solutions - which are readily available to hackers – Netop does not offer a free solution for individual consumers. Focusing entirely on enterprise level solutions and identified customers helps to reduce the chances of Netop's solution being used in cyber attacks.

Furthermore, Netop inherently provides integrated multi-layered security capabilities that not only help staff adhere to corporate policies but also maximize security levels when two or more devices are connected, or attempting to connect, to one another.

What are the potential damages of hacking?

- Loss of data/trade secrets.
- Loss of customer data, including credit card information.
- Millions in fraudulent charges
- A public relations nightmare *

*One Netop customer, a large utility company, estimated a security breach could cost $10,000,000 in potential damages. This seems modest, however, considering that the TJX incident in 2007 cost the company more than $64,000,000.

Netop Remote Control helps organizations by:

Securing the line

Netop allows companies to provide Internet-based remote access through their own servers thereby giving complete transparency and control to the customers and ensuring that corporate security policies are not compromised. Organizations can centrally manage hierarchical connection accounts and govern who can see what, even before the authentication process has begun. This puts a company in complete control of their own data and security.

Netop also provides additional secure connectivity options – including a Netop hosted version – but in all cases remote access traffic uses market-leading 256-bit AES encryption and dynamic key exchange using the Diffie-Hellman method, with key lengths up to 2048 bits to protect your company and your data.

Media Coverage of Remote Access Solutions Used in Hacking Attacks

Hackers use legit remote IT support tool in spy attack

- ZDNET, MARCH 2013

Two charged in theft of $40K from hacked Subway keypads

- CNET, MARCH 2013

How hackers gave Subway a $3 million lesson in point-of-sale security

- ARS TECHNICA, DECEMBER 2011

Managing user access

The target device must impose certain criteria for accepting incoming invitations; otherwise any rogue invitation could allow an intruder access to your network. Managing user access means setting the criteria on which the target device should accept an invitation.

With Netop, this can include any combination of the following:

- MAC/IP Address check. Target devices will only accept invitations from a staff member whose address appears in a predefined MAC/IP list.
- Closed User Group. Assign serial numbers to all service representatives and target devices where only matching numbers may connect. A service representative with any other serial number is rejected.
- Authentication. Netop Remote Control integrates with the authentication scheme deployed at a customer's network – whether this is a Windows Domain, Directory Service, RADIUS server or RSA SecurID server.
- Callback. A target device can call a staff member using a modem, ISDN or TCP connection. This forces the service representative to be at a specific location or machine, another obstacle to prevent intruders.
- User-controlled Access. With this feature, a pop-up window appears on the target device asking the end-user whether they want to accept an incoming request and includes the ID from the service representative. A remote support session cannot be established until the end-user accepts.

Managing user rights

Different remote control users need different access profiles. Companies should be able to define user functionality as needed: lock the keyboard and mouse, blank displays, execute certain commands, transfer files, run programs, manage services, run command prompts, edit registry, etc.

While some high-end remote control products will allow organizations to manage user access rights, not all provide centralized management. With Netop, a company can change the settings for thousands of computers without having to configure each device individually.

Documenting what happened

Netop can provide audit trails for both our hosted and self-hosted connection service allowing customers to track and audit activity. Documentation is the final frontier of a solid secure remote control system. With extensive logging and video recording for sessions, you can know exactly what happened, when. Did the service desk employee delete that important sales file while assisting the sales clerk with his Internet connection? Who remotely accessed the confidential medical records on Saturday night? These are questions companies need to be able to answer and with Netop they can.

Conclusion

Cyber threats are everywhere and the impact of a security breaches can result in significant damages. With the number of devices and connections increasing everyday and number of tools available to hackers – from Shodan to popular and well-known remote access tools – there is a greater opportunity for malicious activity. However, companies can fight back by employing strict security policies and choosing secure remote access solutions like Netop Remote Control.

REFERENCES

1. Hackers use legit remote IT support tool in spy attack

http://www.zdnet.com/hackers-use-legit-remote-it-support-tool-in-spy-attack-7000012949/

2. DataLossDB

http://www.datalossdeb.org

3. Verizon 2012 Data Breach Investigations Report

http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?__ct_return=1

4. Kaspersky Lab Report

http://www.securelist.com/en/downloads/vlpdfs/theteamspystory_final_t2.pdf

Netop

Netop develops and sells software solutions that enable swift, secure and seamless transfer of video, screens, sounds and data between two or more computers over the Internet.

For more information visit: www.netop.com

Netop™ is a trademark of Netop Business Solutions A/S. All other products mentioned in this document are trademarks of their respective manufacturers. The content of this document is subject to change without notice. (1-13)