SECURITY PAPER

NETOP®
Remote Control

Protect Your Data From Ransomware

Ransomware is a potential threat to any business. Although there is no surefire way of preventing a ransomware attack, one can mitigate the risk by following preventive practices and staying informed of vulnerabilities discovered in enterprise software. Vulnerabilities of common tools like remote access support software have been exploited by cybercriminals to spread ransomware through business networks. This white paper describes and examines the main variants of ransomware, types of attacks, best practices of prevention, and the key security functions businesses should consider when choosing the most secure enterprise tools.

Overview: The Problem of Ransomware and Remote Access

Considered to be “the year of ransomware,” 2016 has had its share of these menacing cyber attacks. This pervasive threat continues to victimize businesses large and small; IT service providers, government agencies, retail, healthcare, universities, and financial institutions are prime targets for ransomware. Cybercriminals target those who aren’t properly protected and are mostly likely to give in to their demands. So when a vulnerability is discovered in software that is commonly used across many organizations, a wave of attacks exploiting this particular weakness can be expected to follow.

Recently, cybercriminals discovered that vulnerabilities in widespread remote access tools – such as RDP – could be exploited and used as an attack vector for malware. A great number of companies now find themselves at high risk of ransomware attacks thanks in large part to the ubiquitous presence of remote access tools. Even today, a startling amount of Highly Sensitive Data, including PII, intellectual property, and financial information is left virtually wide open to ransomware attacks because the custodial business neglects to use a remote access tool with adequate security features. Even if the data is returned to the owner, they have no assurance it wasn’t copied and sold on underground markets.

Fox-IT relays why remote access servers have become such popular attack vectors for ransomware: “The power lies in the amount of time the attackers can spend on reconnaissance if no proper detection controls are in place. For example, the attackers have time to analyze how and when back-ups are created of critical company data before executing the ransomware. This helps to make sure the back-ups are useless in restoring the encrypted data which in its turn increases the chances of a company actually paying the ransom” (lindagerrits, 2016).

Before discussing the most effective methods of minimizing the threat of a ransomware attack and protecting your company and customer data, let’s take a step back and dive into the different varieties of ransomware.

What is Ransomware?

Ransomware is a type of malware that covertly installs itself on a victim’s computer, locks them out of their own operating system, and then demands a ransom to return access to the owner.

Why is the threat of ransomware so menacing? First of all, it can access and destroy sensitive data, inflict financial losses, and disrupt business continuity. What’s more, depending on how an organization prepares for and responds to an attack, its reputation and trust can be tarnished forever.

Types of Ransomware

There are two common types of ransomware:

1. **Locker ransomware (non-encrypting)**
   Locks the victim out of the operating system and displays a message requesting payment to unlock it. It is not difficult for a knowledgeable information technician to reverse.

2. **Encrypting ransomware (crypto-ware)**
   Encrypts the victim’s files, in some cases the entire hard drive or Master File Table, making them inaccessible.

Types of Attacks

With new ransomware variants discovered every day, it is critical for organizations to understand the common techniques cybercriminals use to penetrate their victims' machines. Only then can you determine the proper precautions and countermeasures.

These are the most common techniques attackers use to initiate an attack:

- Spam and social engineering
- Direct drive-by-download or malvertising
- Security exploits in vulnerable software such as RDP, VNC, or Teamviewer
- Redirecting internet traffic to malicious websites
- Affiliate schemes/ransomware-as-a-service (RaaS)
- Injecting malicious code into legitimate websites
- Malware installation tools and botnets
- SMS messages (ransomware that target mobile devises)
- Spreading from one infected computer to another

After the malware has penetrated a computer or network of computers, it will remain dormant until the system is most vulnerable then encrypt as much data as possible. The attacker can also add the compromised computer to a botnet to attack additional victims. The owner will be locked out until demands are met: attackers provide an untraceable e-mail address and instructions to pay the ransom in bitcoin.

Who is Targeted?

Cybercriminals target organizations that either deliberately or unknowingly neglect to maintain the proper cyber security standards, which is the overwhelming majority. Attackers take advantage of businesses that use tools and software with known vulnerabilities, e.g. installing ransomware through unprotected remote desktop servers.

Government facilities like hospitals, police stations, schools, and rescue services are popular targets because they simply can't afford the downtime. Their hands are forced to pay the demanded ransom to keep operations on track.

The Anatomy of an Encrypting Ransomware Attack

In order to defend themselves and their customers, security officers and admins need to be familiar with how this notorious threat infects a computer and propagates through networks:

Stage 1: Installation

1. The user visits a compromised website or is scammed by the attacker.
2. The user receives an attachment or link, the malware is downloaded or the attackers exploit a vulnerability on the victim's end, e.g. many business rely on remote desktop functionality, and accordingly cybercriminals will conduct encrypting ransomware attacks using RDP exploits. Attackers breach machines running remote desktop or terminal services via brute force attacks or buying access codes from underground markets. Then they can manually install the malware on the victim's computer.
3. Malware unpacks and executes itself on the compromised computer (or "bot").

Stage 2: Contact & Proliferation

4. The malware contacts the Command and Control (C&C) server to receive the encryption key and/or further instructions.
5. The infected system is used as a launching pad to spread the malware across the network. Ransomware will be dormant until the attackers are satisfied with the number of bots, then the public keys received from the C&C server are delivered to them.

Stage 3: Encryption & Extortion

6. The ransomware encrypts the entire hard disk content using RSA-2048 encryption and uploads encrypted data onto the hacker's temp folder via terminal services client drive mapping file. It can also delete system backups.
7. Once the attackers are satisfied with the amount of captive data, they lock the genuine users out and display a ransom notice with instructions how to pay for the decryption key with bitcoin.

How to Protect Your Data from Ransomware

> *“There’s no one method or tool that will completely protect you or your organization from a ransomware attack, but contingency and remediation planning is crucial to business recovery and continuity - and these plans should be tested regularly”* - FBI Cyber Division Assistant Director James Trainor

Practice Basic Prevention Measures

It’s not uncommon to be left with no choice but give in to an attacker’s demands for payment. In this regard, prevention is your greatest defense.

These are the basic preventive actions you should consider to minimize your chances of an attack:

1. **Regular backups:** Back up data on a regular basis, verify its integrity, and secure all backups. Ensure backups are not permanently connected to the computers and networks they are backing up. Routinely confirm the integrity of your backup copies. Keep in mind, cybercriminals can’t hold your information hostage if you have a copy safely tucked away.

2. **Patch everything:** Patching and keeping your operating system, antivirus, browsers, Adobe Flash Player, Java, remote access, and all other software up to date can prevent compromises and exploits.

3. **Perform regular computer scans:** Ensure antivirus and anti-malware solutions are scheduled to update and scan your computers. Adjust your security software to scan compressed or archived files, if this feature is available.

4. **Disable unsecure remote services:** Consider disabling remote access via RDP or Terminal Services, closing port 3389 and using IP-based restrictions or a VPN. Enable RDP as necessary, and be certain your remote access software meets security compliance standards. Remote access services are well-known attack vectors; cybercriminals are actively searching for unprotected ports used by VNC, RDP, and other common remote access solutions.

5. **Restrict the use of elevated privileges:** No users should be assigned administrative access unless absolutely necessary.

6. **Create a password policy:** Create a uniform password policy for all user accounts with remote access. Set unique, strong passwords for different accounts.

7. **Use application whitelisting:** Only allow systems to execute programs that are known and permitted by your security policy.

8. **Disable macros & scripts:** Disable Windows Script Host, Windows Powershell, macros, and ActiveX. Blocking external content is also a reliable technique to keep malicious code from executing on your machines.

9. **Implement software restriction policies:** Prevent programs in common ransomware locations from executing (e.g. temporary folders supporting popular internet browsers, compression/decompression programs).

10. **Deactivate AutoPlay:** Ensure that harmful programs won’t automatically launch from external media, such as USB memory sticks or other devices.

11. **Educate employees:** Implement and develop security awareness and training programs within your organization, so employees exercise caution with emails, attachments, and downloads.

12. **Choose vendors wisely:** Choose proven vendors and solutions for your sensitive data. Open source software and freeware can make a positive impact in your operations, but when it comes to security and protecting critical data or infrastructure, investing in proven technologies that provide ongoing support and updates is the best way to mitigate risk.

Remember, only an organization that enforces and regularly upgrades security policies and business continuity plans effectively protects their network against these powerful threats.

> *“Organizations should never use weak or default passwords and instead rely on a password policy prepared by CSO (Chief Security Officer) and imposed by IT administration staff.”*
>
> - Dominik Samociuk, IT Security Engineer at Future Processing (Millman, 2015)

Use Secure Remote Control and Access Software

> *“A new strain of ransomware has been discovered that is being circulated by targeted Remote Desktop or Terminal Services hacks.”*
>
> - SC Magazine (Millman, 2015)

This new strain finds cybercriminals penetrating points-of-sale, payment processing systems, data centers, and ATMs by exploiting the vulnerabilities of remote access tools.

> *“Organizations should also consider moving to other remote desktop software if uncomfortable with the out of the box functionality provided by Windows. As with all things Ransomware, the surest solution is a sensible backup plan as no defense is foolproof.”*
>
> - Chris Boyd, malware intelligence analyst at Malwarebytes (Millman, 2015)

To ensure have the strongest defense against ransomware, you must consider these key security features when choosing the right remote control and access solution:

1. **Secure your data:** Sensitive information should be encrypted during transmission to prevent unauthorized access. Choose a vendor that provides 256-bit encryption and dynamic key exchange to protect your company and customer’s data.

2. **Control user access:** Be certain you’re using end-point authentication, i.e. users will be authenticated on each end-point for each session. Only use a solution that allows multi-factor authentication and closed user groups.

3. **Control access privileges:** Access to sensitive data must be restricted by business on a need to know basis. Make sure different users have different access profiles and your remote access solution allows for granular user access management.

4. **Record All Activity:** A comprehensive audit trail must be provided to record and log all events, ensuring that you always know the “who did what” of any remote session. Consider using session video recordings to meet the benchmark of standards compliance.

No safeguard is completely foolproof on its own, but the right combination of preventive actions will significantly lower your risk of a ransomware attack.

Next Steps

Start by assessing the remote access solution at your company. Be sure you're using a solution that exceeds standards for PCI compliance. By taking advantage of advanced security features like multi-factor authentication, activity logging of remote sessions, and customizable access rights, you can keep the benefits of remote access without increasing the risk of a ransomware attack on you or your customers. Talk to us about additional ways to make your remote access system more secure.

Have The Best Security Available

When it comes to remote desktop access and support, Netop Remote Control is the proven industry workhorse. We believe that security and efficiency are not mutually exclusive. Netop Remote Control grants you instant control over keyboard, video, and mouse on nearly every device or OS, while market-leading encryption, multi-factor authentication and activity logging give you peace of mind you won't find from other remote access solutions.

For IT support and help desk, Netop Remote Control is the only choice to comply across all industry security standards. Remotely execute and manage the apps and programs your company needs through secure, on-demand tunnels. Granular control over user rights and privileges allows you to grant secure third-party access into networks and devices within and beyond your local environment.

Consolidating all remote access services into the easy and dependable Netop Remote Control interface simplifies your maintenance and reduces your network vulnerability. This means faster issue resolution, improved workflow, and reduced operating costs.

Click here to read more about Netop Remote Control's security strategy.

Work Cited

Incidents of Ransomware on the Rise (2016, April 29).
https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

lindagerrits. (2016, May 2). Ransomware deployments after brute force RDP attack [Blog Post].
https://blog.fox-it.com/2016/05/02/ransomware-deployments-after-brute-force-rdp-attack

Millman, R. (2015, October 21). Ransomware using Remote Desktop to spread itself.
http://www.scmagazineuk.com/ransomware-using-remote-desktop-to-spread-itself/article/448377/

References

http://www.scmagazineuk.com/ransomware-using-remote-desktop-to-spread-itself/article/448377/

https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962

http://support.eset.com/kb3433/?locale=en_US

https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

http://idt911.com/sites/default/files/uploads/2014/03/030714_Retailer_300ppi-01.png

https://www.markmonitor.com/solutions/industry_solutions-financial-services.php

https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked