Shutterstock: Royalty-free stock illustration ID: 1408742921

Feb 02, 2021 20:26 GMT

Ransoms and beyond

While many organisations had part-time remote working policies in place before 2020, the last year has taken this way of working to a whole new level. In the last year, many organisations hastily implemented changes to their day-to-day operations to support the business requirements without the proper security considerations.

As a result, we have seen threat actors taking advantage of various unsecured and vulnerable publicly exposed remote access solutions, such as Virtual Private Networks (VPN) and Remote Desktop Protocols (RDP).

The following methods and services were found to be commonly exploited as

the main entry point for ransomware attacks:

- Email based phishing attacks / social engineering attacks
- Unsecured VPN solutions
- Remote desktop protocols (RDPs) directly exposed to the internet
    - Password-based attacks (password guessing/brute force attack)

- Web applications with vulnerabilities that can potentially lead to remote code execution on the target's internal network infrastructure

In many cases, ransomware families have evolved their operating model. No longer do these threat actors, including prolific actors such as TA505 (Clop ransomware) and Circus Spider (Netwalker ransomware), just encrypt files (including backups) and extort the victim for payment to get their files decrypted, as is common in traditional ransomware attacks, but they also seek to steal potentially sensitive data from the victim's internal network and threaten to leak them to the public if ransom is not paid.

Threat actors now take advantage of the access that they have on the victim's environment and extract potentially sensitive data such as:

- Personally Identifiable Information (PII)
- Account credentials (username and clear text password or hashes)
- Financial documents
- Company secrets

The ransom note will then contain a link to the ransomware's leak site, which will usually contain instructions on how the ransom can be paid. Usually, the aforementioned blog will also contain information on whether data has been stolen or not.

So, how can organisations reduce the risk of falling victim to new types of ransomware?

Multi-factor authentication

Multi-factor authentication (MFA) is one of the most reliable security features that can be used to prevent an attacker from easily compromising an account with just a username and password pair. A MFA system requires a user to present more than one kind of credential to the system before being successfully authenticated.

The most common type of MFA process involves a combination of a regular password and a One Time Password (OTP), the latter of which is usually generated using a token, or received through a registered mobile number via SMS.

The OTP is usually only valid for a short amount of time before it refreshes, preventing an attacker from gaining access to a compromised account without also gaining access to the token or mobile phone.

MFA should be enabled on all externally facing services such as VPN, RDP, and critical web applications or services.

Security awareness training

The success or failure of a cyber attack all boils down to how the organisation's users tackle security. As such, staff members represent the most critical component in the ultimate success or failure of an attack.

This is why regular security awareness training among staff members is crucial. A good training regime should at a minimum include the following topics:

- Social engineering attacks
    - Phishing
- Scams
- Password security
    - Create strong passwords that are not easily guessable
- Making use of passphrases
- Securely storing credentials
- Malware

- Wi-Fi security
- Data backups
- Reporting to regulatory bodies

Principle of least privilege or zero trust

Users should only be provided privileges that they require for their business functions, and no more. NCC Group's security consultants have discovered that clients' staff members sometimes have excessive privileges which could potentially lead to the disclosure of sensitive information or escalation of privileges.

One scenario involves the access to shared drives; sometimes a user only requires access to one of the folders within the shared drive, but full access to the drive is given. In such a case, if that user's account or credentials are compromised in some way, the attacker will also gain access to sensitive information.

Limiting access will also reduce the attack surface area that a would-be attacker could utilise in order to gain unauthorised access to internal systems and networks.

Keeping software up-to-date

Vendors constantly release security patches and improvements to their respective products. It is security best practice to ensure that all software used within the network infrastructure is free from security vulnerabilities that can potentially be leveraged by threat actors.

Regular offline backup

Once an organisation has been breached, ransomware can typically target anything within the victim's network infrastructure. This include backups that are directly accessible within the network. The best way to combat this and avoid potential loss of a large amount of data is to keep regular offline backups. The most robust solutions include fixed media backups at a regular interval that is feasible with the organisation's risk appetite, or use isolated as-a-service models such as data escrow.

Audit log collection and retention

Ensure that logs from critical services and networks are securely kept and stored for at least 90 days, but ideally years. This source of information will be immensely helpful in the investigation as well as identifying the activities performed by the threat actor.

Logs from the following sources are highly recommended to be retained:

- Remote access logs
- Proxy logs
- Authentication logs
- Process creation including command line parameters
- DNS requests

Feeding this information into a Security Information and Event Management (SIEM) system is also recommended for centralised log management or to a third-party Managed Detection & Response providers.

Resilience via defence-in-depth

No single security solution is a silver bullet in the ongoing fight against threat actors. Defence-in-Depth security is always the best practice approach. Multiple layers of security, training and process will ensure that when one layer of security has been compromised, another layer comes into play to help defend the organisation's resources.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and

manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970