LRQA NETTITUDE

Breaking Attacker Playbooks

Pragmatic and realistic defensive improvements

Doug McLeod & Tom MacDonald

13th September 2023

Contents/Agenda

- Introduction – The **WHY**
- Key Themes Overview – The **WHAT**
- Key Themes in Detail – The **HOW**

- Q&A – don’t wait until the end!

Introduction

"Fundamentally, if somebody wants to get in, they're getting in...accept that.

What we tell clients is number one, you're in the fight, whether you thought you were or not.

Number two, you almost certainly are penetrated."

-- Michael Hayden, Former Director of NSA and CIA

Introduction

- Aim to highlight realistic and pragmatic improvements that will prevent attackers gaining quick wins in your environment.
- The ‘base standard of maturity’ and public / regulator expectations have increased – organisations must continue to evolve to keep pace.
- Technical fixes represent a point-in-time moment, and patching is only part of the solution – increase organizational resiliency and actively plan for a compromise.
- These controls and detections drastically reduce our success rate across all types of red team scenarios – supply chain, malicious insider, devops pipeline pollution, external attacker.

Methodology

Thematic Red Team Results

- 90% of our recent attacks did not exploit any typical vulnerabilities that would be resolved through patch management.
- 40-50% of Red Teams have some direct attack on Active Directory or AzureAD, often centred around Active Directory Certificate Services or SCCM.
- Extended recon is critical: Confluence, Jira, ServiceNow, File Shares, Git / BitBucket…etc.
- NTLM relaying and machine coercion are featuring in more and more attack paths. This will filter through to other malicious actors over the coming months.

“I’ve got an EDR, a proxy, a DLP solution and an MFA VPN – I’m all compliant and safe!”

Key Themes

LRQA NETTITUDE

Key Themes

High Level Overview

- Controlling the Network
- Defence in Depth
- Customised Detection Rules & Low Hanging Fruit
- Perimeter Controls
- Empowerment to Act

Key Themes

Controlling the Network

- Prevent workstation to workstation communications – VPN client isolation & local firewalling rules drastically reduce lateral movement opportunities.
- Servers should usually have 4 network interfaces for different traffic
  - 2 x access plane
  - 1 x management plane
  - 1 x backup plane.
- Deploy EDR to all hosts without exception, along with Attack Surface Reduction rules.
- Check your M365 licencing – E3 & EMS or E5 includes Microsoft Defender for Identity.
- Force the administrators to use approved tools rather than preference– you can detect abnormalities via use case development.
- The foundation of enterprise security is enterprise systems administration; poorly trained IT teams lead to poor security outcomes.

Key Themes

Defence in Depth

- Back to Front and Front to Back defences.
- Attacks do not only come from the perimeter.
- Dedicated Application-Layer logs for authentication and privileged / sensitive actions.
  - How do you track and detect user activity in your critical applications?
- Protect your critical systems with MFA and Layer 3 segregation
  - Host based firewalling for critical servers are quick wins and scale well.
  - Firewall your critical database servers from Layer 3 access apart from Jump Host and App Servers.
- Jump Hosts and separate tiers of accounts for administrators are essential and non-negotiable.
  - Implement Remote Credential Guard on Windows 10/11 and make use of WinRM / PowerShell remoting.
- Whilst patching is important, don’t focus to the detriment of other activities. Organisations focus on it because it is easy to measure and show value to the business.

Key Themes

Customised Detection Rules & Low Hanging Fruit

- Attackers can buy your EDR and trade bypasses and novel techniques in closed communities – if you are running vanilla EDR (without a dedicated MSSP or similar) then it **will** be bypassed.
- All EDRs are not equal – but nor are all MSSPs – look for services that offer additional threat hunting services. MSSPs can be responsible for maintaining the security of the environment, but not the accountability.
- Example detection:
  - RDP TCP/3389 traffic not originating from mstsc.exe or SSH TCP/22 traffic not originating from Putty or other approved apps.
- Carry out focused Active Directory/ AzureAD reviews – it requires dedicated phase in internal penetration testing.
- Application allowlisting without complementary detective rules is ineffective.
  - wscript / jscript / hta / vbs / vba / xll from user-writeable directories

Key Themes

Perimeter Controls & Proactive Defenses

- Sandbox macros and executable file types at the email layer – sandboxing technology must simulate being domain joined.
- Stop non AzureAD-*registered* devices from accessing M365 – reduce Evilnginx attack severity.
- Web Browsing Isolation and Content Detonation Technologies are high effort but high reward changes.
- Honey credentials in file shares / Jira / Confluence – linked to high fidelity and low false positive alerts in SIEM.
- Manually scrape your own document repositories for credentials. Crack your own passwords and continually scrape.
- Staff who can self-elevate accounts (cloud or on-prem) are an extreme risk.
- Scrutinise your business – what cloud providers and services do you use? Only permit those services.

Key Themes

Empowerment to Act

- Cannot defend the company in isolation – will require IT Ops / Regulator Engagement / Marketing. Relationships will get strained under high pressure, and it will need robust leadership to ensure all parties are pulling in the same direction.
- Find time to study and rehearse your IR plans – you will fail to level of your training.
- Continuously refer to *MITRE 11 Strategies of World Class SOC* to benchmark yourself against industry leaders.
- Reduce the cost of table top exercises by each staff acting 'one level up' or accepting less-than-full attendance – replicate the most likely attendance.
- Must be empowered to make disruptive changes in order for the wider business to survive.
- Playbooks are authority to act, not flowcharts.

Conclusion

- A lot of attackers are after quick wins and multi monetization – but not all.
- Removal of low hanging fruit should be an ongoing process, not limited to annual pentests.
- Baselining the environment and understanding normal user behaviour is essential.

- Prepare for the breach in advance and actively train the rest of business on their roles. Let your red team play out until it hurts.
- Manage the expectations of the executive leadership about your capabilities.
- Be prepared to make the difficult decisions based on the limited information you have.
- Having configuration as code for servers and loosely coupled components will drastically reduce the time to restore P1 applications.

Q&A

LRQA
NETTITUDE

Actionable Today

- **Delivery** - Downloading Files / HTML Smuggling - Web Isolation POC
- **Execution** - Application Control List and buy detection rule pack.
- **Reconnaissance** – Proactive scraping of fileshares/repos and excessive honeycreds.
- **Lateral Movement** – Segregation, Firewall Workstation to Workstation and Server to Workstation (WMI, WinRM, SMB, RDP).
- **Comms** – Control servers at Layer 3 to only reach dedicated proxies that permit only EDR-telemetry URLs.
- **Comms -** Disable recursive DNS from endpoints and non-resolvers.
- **Acting on Objs** – Stop SSH / DB access from non-Jump Boxes.
- **Acting on Objs** – Change Management for GPOs will stop or detect many ransomware attacks.

Something is better than nothing. Don’t accept the ‘that won’t work / too difficult’.