Top of the Pops: Three common ransomware entry techniques

research.nccgroup.com/2022/08/04/top-of-the-pops-three-common-ransomware-entry-techniques

August 4, 2022

by **Michael Mathews**

Ransomware has been a concern for everyone over the past several years because of its impact to organisations with the added pressure of extortion and regulatory involvement. However, the question always arises as to how we prevent it. Prevention is better than cure and hindsight is a virtue. This blog post aims to cover some high-level topics around ransomware groups, affiliates and their initial entry tactics.

Something to consider is the fact that ransomware has moved quickly into a Ransomware as a Service (RaaS) model, whereby affiliates are being provided all the weaponry and playbooks required to carry out their objectives. Given the simplicity of this approach, and the

fact that the tactics are repeatable, there are a number of preventative measures that can be taken. Using this, we have devised this blog post to provide a short list of the top initial entry methods observed from the front line whilst responding to incidents over the past 6 months.

ProxyShell

ProxyShell is the collective name used to describe the vulnerabilities, released between April and July 2021, affecting Microsoft Exchange. This vulnerability has been covered in detail elsewhere [1], therefore for conciseness, they can be summarised as:

- ACL Bypass (CVE-2021-34473)
- Privilege Escalation (CVE-2021-34523)
- Remote Code Execution (CVE-2021-31207)

Due to the Exchange infrastructure being externally facing, affiliates cast their nets far and wide scanning for victims that have failed to patch and thus begin their attacks by using ProxyShell as their initial foothold.

Mitigations

- KB5001779
- KB5003435

Patching! Patches were released in May 2021 by Microsoft to mitigate the vulnerabilities in the form of Windows update codes:

Microsoft Exchange Online or Office365, as more commonly referred to, was not affected. SaaS is a well placed alternative and provides a barrier to your on-premises network (with appropriate security controls).

Externally Facing Infrastructure

Whilst we could classify Exchange under this term, it deserved its own spot given it is a firm favourite with ransomware groups (partly due to its success rate). In this category, we will cover another favourite, specifically referring to firewalls.

FireWalls and other perimeter security solutions have grown ever more complex and offer a wide variety of services outside of allowing and denying network traffic on the perimeter, most notably VPN’s.

A prime example of this is a vulnerability that was exploited in FortiGate devices, CVE-2018-13379. The vulnerability itself was directory traversal but, it did provide access to sensitive files which contained plaintext passwords. In turn, you have your recipe for disaster and a ransomware actors initial entry point. The username and password could be used to

authenticate with the VPN and gives threat actors a foothold on the internal network. However, this is just one example, on several occasions we have observed firewalls being targeting and successfully leveraged as an entry point into the network.

Mitigations

Once again patching, edge network devices are extremely vulnerable given their position within the network, the precise device you are using to keep threat actors at bay may in fact be the target in the first place. Ensure you have a robust patching policy, and your devices are updated frequently.

Second, multi factor authentication (MFA) is critical to mitigate standard username/password-based attacks. Although a vulnerability is exploited to gain access to credentials in this instance, phishing would have had the same impact if VPN credentials were targeted.

Exposed Remote Desktop (other VDI solutions)

An old favourite, the GUI interface of RDP. Whilst a great way to connect to a remote device, it does not really have a place on the internet. If you are seeing your failed login count hit numbers you cannot easily say, there may be an underlying problem that could be a host exposing RDP to the internet.

When paired with weak security controls, weak credentials (domain or local), no lockout policy, you are effectively providing a free shot to affiliates to take a gamble and gain access to your network. This is most prominent with development environments, setup with default settings, a weak local password and publicly available for ease of use. This is especially prevalent in cloud environments where build images inherit several security flaws through poor configuration but allow users to stand up infrastructure quickly.

Mitigations

Use a enterprise VPN solution with MFA configured to access internal resources from remote locations.

Treat development environments with care and ensure build images have appropriate security controls and protective monitoring in place.

Proactive Measures

Taking a proactive stance to ensure the integrity of your network is critical, it is never too late to begin to harden your defences or at least verify you are secured. However, if you need support or help to assess the scale of the issue, we can help:

- Unsure if you are affected by any of these vulnerabilities or misconfigurations?

- You have identified a host that is vulnerable is requires further investigation?
- Concerned about what is lurking in the wider network?

If you have been impacted by any of these issues, or currently have an incident and would like support, please contact our Cyber Incident Response Team at +44 161 209 5148 / cirt@nccgroup.com

[1] https://www.ncsc.gov.ie/pdfs/MS_Proxyshell_060921.pdf`