Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Malicious Cyber Activity Targeting Information Technology Managed Service Providers

FOR MANAGED SERVICE PROVIDERS AND THEIR CLIENTS

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

1 BACKGROUND

The Canadian Centre for Cyber Security (Cyber Centre) is aware of the ongoing malicious cyber activity targeting information technology (IT) managed service providers (MSPs) and has been providing advice and guidance to Canada-based MSPs and Canadian businesses who use MSP services.

Since at least May 2016, the threat actors responsible have used various tactics, techniques, and procedures (TTPs) to compromise a number of major global Managed Service Providers (MSP), and have successfully obtained sensitive client information. This activity has affected MSPs and their clients around the globe.

The Cyber Center notes that this particular threat actor is not alone in using trust relationships to compromise victims and the recommended mitigations to reduce risk can be applied more broadly.

1.1 WHAT IS AN INFORMATION TECHNOLOGY (IT) MANAGED SERVICE PROVIDER (MSP)?

MSPs[1] are companies that offer a range of information management and information technology services. This includes physical, virtual, or cloud infrastructure, as well as providers who manage stored data primarily in a virtual environment.

Organizations are increasingly relying on MSPs to provide a range of IT infrastructure and support services. The business decision to outsource a company's IT computer support network and management may be an alternative to hiring in-house IT specialists, or to allow an organization to focus on business operations. From a security standpoint, MSPs have the potential to reduce the risks that could occur with in-house IT development in enterprises that do not have the resources or experience to develop secure one-off solutions.

1.2 WHY ARE MSPS TARGETED?

MSPs are an attractive, high-value target for threat actors. This is because MSPs typically have extensive access to multiple client networks in order to perform their job of IT specialist. The compromise of one MSP can affect multiple clients globally and provides a threat actor with access to multiple client systems and sensitive data, leading to loss of proprietary information, disruption to business operations, financial loss, and potential harm to the affected organization's reputation.

In order to successfully compromise an MSP, a threat actor infiltrates it using varying means, such as deploying sophisticated malware for remote access. In some instances, the malware deployed by a threat actor has the ability to both evade detection and maintain persistence on an affected network. Once the threat actor gains a foothold in the MSP's network, tools are used to steal legitimate credentials, including system administrator credentials. After MSP administrator credentials are obtained, malware may no longer be needed because common network management tools trusted by client systems provide better cover for the cyber-intrusion. Clients of interest to a threat actor can then be accessed via MSP accounts and network interfaces. Data can then be compressed, staged for removal, and exfiltrated through the MSP, or through client infrastructure, back to the

[1] Managed service providers (MSPs) also include cloud service providers (CSPs) in the context of this document.

threat actor’s infrastructure. MSP clients with a high security posture are less likely to notice data going to an MSP than directly to the Internet, and MSP clients with a low security posture can be used as exfiltration points.

2 THREAT MITIGATION AND ADVICE

There is no singular mechanism or solution to protecting and defending a network, and the Cyber Centre recommends employing multiple, layered defence measures and actions for the best results.

Some traditional cyber security measures, such as use of firewalls, may not be effective in this scenario. However, there are mitigations available to guard against insider threats, or the risks of compromised credentials, which are worth highlighting here.

1. Google publicized that after implementing two-factor authentication for all employee accounts, no successful phishing activity was conducted against their corporate servers[2]. This is evidence that multi-factor authentication (MFA) helps to limit phishing attacks, which are a common vector used to deliver the malware for network infiltration. MFA also inhibits cyber-actors from gaining free access to information once inside networks, since stored credentials that a threat actor might find are useless, in a secure network, without at least a physical second factor.

   - MFA is advisable for all system users, but it is especially advisable at system connection points that would be accessible to MSPs and teleworking employees. Logs from these connection-point servers should be segregated, centralized and regularly reviewed.

2. Automated Behavior Analysis tools can profile the IT needs and habits of employees on the corporate network, detect deviations from normal patterns, and generate appropriate alerts. Behavioral analysis software could identify threat actors posing as employees with valid credentials, as their activity could deviate from the employee’s regular pattern of IT use.
3. The Cyber Centre recommends using Privileged Access Management solutions to control when access to client systems is granted and when it is taken away. Reviewing logs to reconcile access to client networks with authorized tasking needs to be performed regularly.
4. Report all suspected compromises as soon as possible to the Cyber Centre at contact@cyber.gc.ca for confidential advice and guidance.

SPECIFIC ADVICE AND GUIDANCE TO MITIGATE MSP RISKS

Below are steps that MSPs and/or their clients can take in combination to increase the likelihood of detection, and to decrease the likelihood of a successful compromise. The Cyber Centre recommends MSPs and their clients review the following mitigation advice and consider their implementation in the context of their network environment.

2.1 FOR IT SERVICE PROVIDERS (MSPS)

The *modus operandi* of this threat actor — gaining access to legitimate credentials on one network to access client data on another — presents a challenging problem for trusted service providers. The Cyber Centre recommends all MSPs adjust their security posture in the following areas to limit the success of this threat actor. The anticipated

[2] Google use of hardware-key based 2 factor authentication neutralized employee phishing https://krebsonsecurity.com/2018/07/google-security-keys-neutralize-employee-phishing

publicity surrounding the current news release will likely cause MSP clients to seek the MSP's advice, and the following guidance should aid those discussions.

2.1.1 ACCOUNT CONTROL

- Limit the ability of a local administrator account to log in from a local interactive session (e.g. "Deny access to this computer from a network") and do not allow access via a Remote Desktop Protocol session.
- MSP employees who carry out administrative functions with clients should use unique, strong passwords for access to client networks and for each client for which they have responsibilities. Passwords should be reset on suspicion of or indication of compromise, and wherever possible should be supplemented by MFA.
- Mechanisms such as Privileged Access Management solutions should be deployed to ensure access to administrator accounts and client accounts is time-limited, logged and validated against approved requests.

2.1.2 NETWORK SECURITY

- Client management zones within the MSP should be separated to limit lateral movement between them.
  - Firewall rules should be reviewed and adjusted to control how whitelisted connections from the MSP to the client, the client to the MSP, and between the MSP management consoles are managed.
- If VPN is used for client network access, these interfaces should be carefully scrutinized for unusual activity and verbose logging should be instituted.
- Implement logging on DNS servers and monitored for abnormal patterns of DNS behavior, especially dynamic-DNS domains.
- Avoid enabling remote management over the Internet and using default IP ranges.
- Automatically log out after configuring routers.

2.1.3 WORKSTATION MANAGEMENT

- Hosts with confirmed compromises should be removed from the network for forensic analysis.
- The number of cached credentials should be reduced to one if a laptop, or zero if a desktop or fixed asset.
- Review anti-virus scan results on a regular and ongoing basis.
- Management workstations (either through hardware separation or virtualization) should be dedicated to each client.
- For workstations that hold MSP or client administrator credentials, the number of Internet-facing applications should be minimized or removed entirely, as each of these applications are a potential vector for compromise.

2.1.4 SERVER MANAGEMENT

- Do not use cached credentials.
- Workstations used to administer servers or infrastructure devices should not be used for general internet browsing/access.

2.2 FOR CLIENTS OF MSPS

MSP clients have a responsibility to ensure appropriate security mechanisms have been selected to control access to their systems, whether for an employee, administrator, or MSP administrator. Granting remote access should be done with the same vigilance one would apply when granting physical access to systems and their sensitive information. The Cyber Centre recommends all clients of MSPs seek to strengthen their security posture.

2.2.1 CONTRACTING WITH AN MSP

- Ensure an MSP solution satisfies *in writing* the organization's security, privacy and legislation requirements.
- Ask how data is being segregated from that of the MSP and other client organizations.
- Ask how the MSP protects the accounts of network administrators with access to proprietary data from being impersonated by a threat actor.
- Determine how long the MSP keeps logs of their activity, the level of detail of those logs, how the logs are protected and if the logs are centralized.
- Ask what notifications the MSP will provide in the case of compromise of their systems and particularly of administrative credentials.
- Ask what patch management practices the MSP will adhere to in order to minimize vulnerabilities.
- Establish lines of communication, separate from corporate networks, that will be used in the event of a compromise of the organization's or MSP's corporate networks.

2.2.2 CONTROLLING MSP ACCESS

- Avoid providing the MSP with account credentials and/or access to sensitive systems outside of their responsibility.
- Consider implementing MFA (e.g. security tokens for remote access to any sensitive data repositories) and a strong password policy across the organization, starting with administrator/privileged accounts.
- Consider mitigating potential exploitation by monitoring vulnerability scan results and following a prioritized and responsive patching cycle to keep all operating systems, applications, software, and third-party software up-to-date with the latest patches.
- Consider reducing and monitoring the number of domain and enterprise administrator accounts.
- Monitor anti-virus scan results and other network logs for suspicious activity on a regular basis.
- Employ a data backup and recovery plan for all critical information.

2.3 OTHER CONSIDERATIONS

There are other considerations, which are not specific to this compromise, to take into account when engaging with an MSP:

- Consider factors such as who owns the data, where the data is stored, how it is backed up and what security measures are in place.
- Consider asking any service provider to what extent they adhere to an IT security management framework. See *"Cyber Centre's IT Security Risk Management: A Lifecycle Approach (ITSG-33)"*
- Use cryptographic controls to protect data in transit between the client organization and the provider.

3 RESOURCES

For a more detailed list of guidance and best practices, and for additional information, please consult the following publications previously issued by the Cyber Centre (under CCIRC) and our international partners.

Cyber Security Best Practices: Contracting With Managed Service Providers (IN-17-003)

https://cyber.gc.ca/en/guidance/cyber-security-best-practices-contracting-managed-service-providers

Malicious Cyber Activity Targeting Managed Service Providers (AL17-004)

https://cyber.gc.ca/en/alerts/malicious-cyber-activity-targeting-managed-service-providers

Using Passwords

https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-dntty/usng-psswrds-en.aspx

Get CyberSafe Guide for Small and Medium Businesses

https://getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-en.aspx

Cyber Centre's IT Security Risk Management: A Lifecycle Approach (ITSG-33)

https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33

NCCIC – Advanced Persistent Threat Activity Exploiting Managed Service Providers (TA18-276B)

https://www.us-cert.gov/ncas/alerts/TA18-276B