Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Investigation Report: Compromise of an Australian Company via their Managed Service Provider

cyber.gov.au

Compromise of an Australian Company via their Managed Service Provider

Introduction

1. Managed Service Providers (MSPs) are attractive targets for state actors and cybercriminals. This investigation by the ACSC is one example of how Australian organisations are at risk of commercial secrets, data and information theft via their MSP. This report details an ACSC investigation. It includes technical findings and mitigation advice related to the compromise of the Australian arm of a multinational construction services company via their MSP.
2. The tactics, techniques and procedures (TTPs) observed in this compromise align with a public report titled "Operation Cloud Hopper"[1], which details APT10's targeting of MSPs to leverage existing trust relationships with their customers and gain access to their customer networks.
3. For mitigation strategies to manage the security risks posed by engaging and authorising network access to MSPs, the ACSC recommends reviewing the PROTECT product *How to Manage Your Security When Engaging a Managed Service Provider*[2].

Investigation Summary

4. In March 2017, the ACSC received a report that indicated a computer belonging to the Australian arm of a multinational construction services company (hereafter the victim) was compromised with specific malware. The malware associated with the activity was previously publically attributed to the threat actor known as APT10[3].
5. The ACSC engaged with the victim to investigate malicious activity involving this malware. The investigation developed an understanding of the malware, associated tradecraft, and any actions performed by the actor. This information then enabled the victim to successfully remediate the activity. The victim also engaged a third party security incident response provider to assist with remediation of the compromise and help implement strategies to improve the overall security resilience of the victim's network.
6. The investigation revealed that the malware was a variant of the well-known "PlugX" Remote Access Tool (RAT). The compromise occurred using an administrator account provisioned legitimately to one of the victim's MSPs. This account was utilised by the malicious actor to remotely connect from an IP address allocated to the MSP into the victim's network and install the RAT.

[1] https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf
[2] https://www.cyber.gov.au/publications/how-to-manage-your-security-when-engaging-a-managed-service-provider
[3] https://attack.mitre.org/wiki/Group/G0045

Targeting

7. In this investigation, the successful compromise of a MSP by APT10 was utilised to access sensitive data and commercial secrets held on MSP customer networks (see Figure 1)

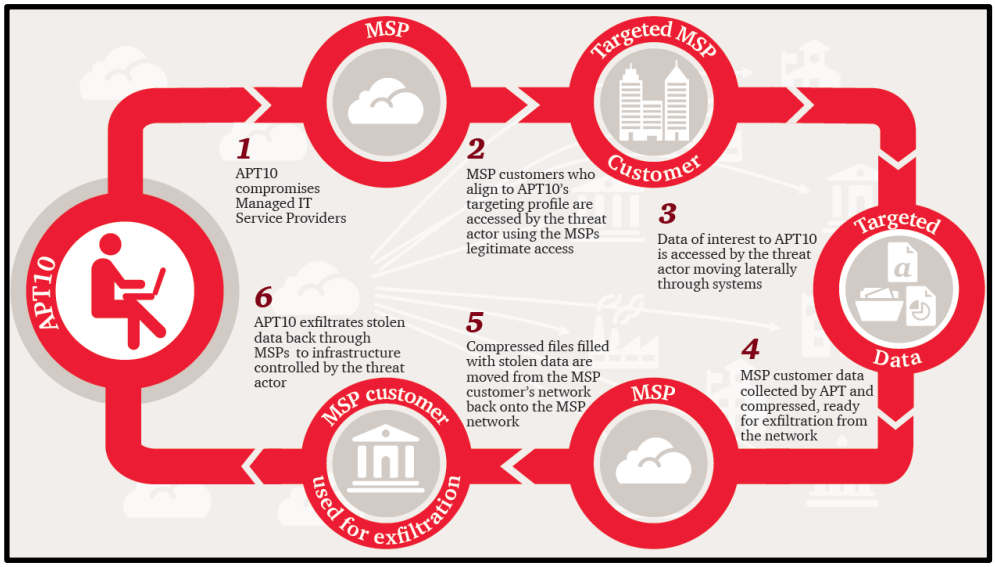

Figure 1: AP10's targeting methodology. APT10 targeted MSPs to leverage existing trust relationships with their customers and gain access to their customer networks. Image sourced from Operation Cloud Hopper Report[1].

Key Technical Findings

8. The earliest evidence of compromise was identified on a read-only domain controller, DC-1. On 19 September 2016, a legitimate support account provisioned to a MSP logged on to this server via a remote desktop connection from an IP address allocated to the MSP. 25 seconds after interacting with the server, PlugX malware was installed as a service named "Corel Writing Tools Utility". FireEye attributed similar activity to APT10 in their April 2017 "MenuPass" report[4].

9. Between October 2016 and early November 2016, the PlugX malware was installed on four additional workstations in the victim network: WK-1, WK-2, WK-3 and WK-4. The PlugX malware was also re-installed or updated on the DC-1. In all cases, the malware was installed as a service, sometimes named "Quick CreateInstall Installer".

10. On 8 November 2016, a listing of Active Directory domains, trusts, users, groups and computers were saved to WK-2. The data was stored in text files and compressed as a Cabinet type archive (.CAB). The data did not contain any passwords, but enabled the actor to understand the users and computers of the wider global corporate network.

[4] https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

11. On 25 November 2016, an NT Directory Services (NTDS) file from another domain controller, DC-2, was stored on WK-4. This file was unrecoverable, but the NTDS file is the Microsoft Active Directory database file that contains all corporate user and computer account details, including encrypted passwords. This file could be easily decrypted by an actor and then used to log into the network via legitimate remote access such as a Virtual Private Network (VPN). At this time, PlugX is also believed to have been installed on DC-2. DC-2 was one of few globally writable domain controllers. This would enable an actor to maintain persistence on a server which was capable of modifying the Active Directory users and groups.
12. On 23 December 2016, PlugX was re-installed as a service named "SAP Quick Installer" on WK-4. This host was then used to conduct the majority of future malicious activity.
13. On 4 January 2017, the actor "parked" some of their infrastructure. This activity was identified when the malware command and control (C2) domain began resolving to IP addresses 0.0.0.0 or 1.1.1.1.
14. On 25 April 2017, a new malware variant known as RedLeaves[5] was installed on WK-4, replacing the previous PlugX malware[6]**.** This may have been a reaction to public reporting, as it occurred three weeks after the announcement of Operation Cloud Hopper. The actor utilised the InstallUtil technique[7] to potentially bypass host defences.
15. On 3 May 2017, another listing of Active Directory CSV text data was saved to WK-4, providing the actor with an updated view of the organisation's network.
16. On 4 May 2017, the actor installed the new RedLeaves malware to the previously compromised workstation WK-1 and newly compromised WK-3.
17. On 8 May 2017, a publically available post-exploitation tool called Mimikatz[8] was executed on WK-4, indicating a further attempt to acquire cached credentials from the workstation.
18. Between the 9 and 12 May 2017, the actor installed suspicious software from WK-4 on two read-only domain controllers in another country, DC-3 and DC-4. WK-4 was also used to remotely access 12 other servers and workstations within and outside of Australia.
19. On 22 May 2017, the actor deleted evidence from WK-4, the host where the majority of malicious post-exploitation lateral movement activity had originated.

Mitigation Strategies

20. This section details the mitigation recommendations provided to the victim. These were in addition to the advice and remediation actions undertaken by their third party security incident response provider, to improve the overall security resilience of the victim's network.
    a. **Increased logging** to improve visibility of victim's systems. It is advised that logs be retained for as long as possible; based on the incident timeframe, a minimum of 18 months logging would assist with any future incident investigations[9]. This includes but is not limited to network gateway logs, host event logs and remote access logs.

[5] https://attack.mitre.org/wiki/Software/S0153
[6] https://attack.mitre.org/wiki/Software/S0013
[7] https://pentestlab.blog/2017/05/08/applocker-bypass-installutil
[8] https://attack.mitre.org/wiki/Software/S0002
[9] https://www.cyber.gov.au/publications/windows-event-logging-and-forwarding

b. **A software patching policy** will assist in maintaining up to date versions of software, which assists in decreasing the risk of network compromise[10].

c. **Application control** will allow only essential services and applications to run and prevent malicious software from executing on a network[11].

d. **Restrict Administrative Privileges** can decrease the chances malicious threat actors have of gaining privileged access to the victim's network[12]. This includes separation of duties and ensuring staff members can only log in to administrator accounts when administrative authority is required.

e. **Enable multi-factor authentication** on remotely accessible services, such as virtual desktops, VPN and web based email[13]. This will ensure that even if an actor has compromised credentials, they still cannot log on without a second factor such as a hardware token.

f. **Segment networks** to limit an adversary's ability to move laterally within a network[14]. Consider segregation from both a regional and resource perspective, for example, which networks or workstations can directly connect to one another and/or to servers.

g. **Utilize a secure jump host** to perform administrative tasks. Specify a dedicated workstation where managed service providers and administrative staff can perform sensitive administration duties, with restricted access to critical servers. Combine with multi-factor authentication to limit an adversary's ability to compromise critical assets.

h. **Implement the ACSC Essential Eight**, a prioritised list of strategies to mitigate Cyber Security incidents developed by the Australian Signals Directorate[15]. These strategies are effective in defending against malicious activity such as preventing the execution of malware and reducing the attack surface of an organisation.

[10] https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches
[11] https://www.cyber.gov.au/publications/implementing-application-control
[12] https://www.cyber.gov.au/publications/secure-administration
[13] https://www.cyber.gov.au/publications/implementing-multi-factor-authentication
[14] https://www.cyber.gov.au/publications/implementing-network-segmentation-and-segregation
[15] https://www.cyber.gov.au/publications/essential-eight-explained