Password Spraying and NSO Groups: A look into Iran’s Cyber-soldiers

Ever since its inception, the United States of America has had a myriad of foreign adversaries. Starting in 1980, after the severing of diplomatic relations, one of those foreign persistent threats became the nation of Iran (United States Department of State, 2023). In September of 2023, a new report from big tech company Microsoft, detailed an apparent cyber campaign against U.S companies and government agencies that appeared to be from the Iran-backed cyber warfare group “Peach Sandstorm” also known as APT33, Elfin, Holmium, and Refined Kitten (Microsoft Threat Intelligence, 2023).

According to Microsoft, this nation-state actor has been engaging in this cyber campaign since February of 2023. Peach Sandstorm has been involved in this sort of cyber sortie to advance Iranian state interests by way of intelligence collection. They have gone after organizations that are usually encompassed by the sectors of education, energy, aviation, telecommunications, finance, and any other country mission critical sectors. Their prime attack pattern was mainly what most cybersecurity experts consider “brute forcing.” Instead of the main style of brute forcing which usually involved obtaining a list of passwords to try and putting it through some type of tool or software to hyper-fixate on one account or target service, this group used a method called “password spraying”, where they used their obtained list of passwords to “spray” or “try” one password at a time across multiple accounts.

Peach Sandstorm’s intrusion chains observed by Microsoft followed one of two paths, however both ultimately ended in the group trying to exfiltrate data from the target organization. The first path was initiated with the preeminent password spray attack. When that availed and root access was obtained by moving laterally, they would do network reconnaissance by using AzureHound or Roadtools. AzureHound is a Go-based binary that can collect data from Active Directory (now known as Microsoft Entra ID) in Azure cloud environments through the use of REST APIs or otherwise known as RESTful APIs. RESTful APIs serve as a communication interface between computer services or endpoints that allows for the successful transfer of information in a multitude of formats. Roadtools is a more sophisticated version of AzureHound providing a much broader and more extensive suite of tools for network reconnaissance. It serves as a framework to enter an organization’s Microsoft Entra ID (Microsoft Threat Intelligence, 2023). As an alternative to those methodologies, they instead create a new Azure subscription on the host’s system and use it as a way to compromise other Azure resources. In this path, Peach Sandstorm also made sure to make use of Azure Arc. Azure Arc is a remote cloud environment management solution for Azure cloud environments. Peach Sandstorm would put Azure Arc onto their compromised subscription and proceed with their malicious endeavors from there. What made this plethora of tools so devastating was that it allowed for them to remotely control on-premises target devices connected to the network.

While the former attack path or pattern seemed to be heavily focused on anything that was Microsoft-based, their second path would have a comprisal of abusing publicly known vulnerabilities in Zoho ManageEngine or Confluence. ManageEngine was basically the Zoho equivalent to Microsoft's Azure Arc, and Atlassian's Confluence followed suit. The two main vulnerabilities that the nation-state actor abused were CVE-2022-47966 and CVE-2022-26134. CVE-2022-47966 is a remote code execution vulnerability that, when put into use, would affect a group of on-premises ManageEngine solutions. After coming to the knowledge of this vulnerability, Microsoft made sure to patch it and implore organizations to update their systems to ensure that the patch was now put into effect. CVE-2022-26134 happened to be the same type of vulnerability except it would go after Confluence Server and Data Center. Server and Data Center in Confluence made it so that an organization's cloud infrastructure was managed by Atlassian. The discovery of this vulnerability led Microsoft to release a report detailing recommendations to mitigate and defend against it. Essentially some system hardening tips.

Although the group Peach Sandstorm attacked a variety of sectors, a substantial amount of activity following the compromise of the targeted system was seen in cases where the target was a part of the defense, satellite, and pharmaceutical sectors. To maintain persistent access to many of their targets in this arena, they deployed AnyDesk, a monitoring and management solution that could be used off-premises remotely (Microsoft Threat Intelligence, 2023). The use of AnyDesk was a very lucrative choice for many instances since the software was already legitimately being used by a deluge of these organizations that were in their crosshairs. It allowed for greater obscurity of Peach Sandstorm's operations on the compromised network and system. Another form of maintaining access into a target system was through the use of what is called a Golden SAML attack. This type of attack would consist of a malicious actor stealing private keys from the target organizations AD FS (Active Directory Federated Services) server and then using those private keys to create for themselves a SAML token that could then be used to bypass the usual security locks in a Microsoft Azure environment. Private keys are used in tandem with an algorithm for the cryptography of data. SAML keys or otherwise known as Security Assertion Markup Language keys are keys that are produced in XML-based format for user authentication between internal company domains. But in another group of attacks, the Peach Sandstorm group implemented EagleRelay to tunnel all network traffic back to their servers and infrastructure. The threat actor would create virtual machines using their compromised Azure subscription and then run EagleRelay to exfiltrate data (Microsoft Threat Intelligence, 2023).

Although this group has really gained notoriety in 2023, their attacks of the aforementioned types still do persist today in 2024. They are continuously developing better and more advantageous ways of compromising systems and networks and will continue to do so. Even in December of 2023, Microsoft warned of another Backdoor called "FalseFront" in which the threat actor had companies and organizations in the DIB or Defense Industrial Base in its crosshairs. According to the Microsoft Threat Intelligence Twitter profile, “Falsefront is a custom backdoor with a wide range of functionalities that allow operators to remotely access an infected system, launch additional files, and send information to its [command-and-control] servers.” Although research pieces came out about this backdoor and persistent threat medium in December, November was when the first utilization of it was seen.

Another group that has been involved in similar activity such as Peach Sandstorm is a group named PHOSPHOROUS. PHOSPHOROUS, also an Iranian nation-state actor, has been going after targets similar to the likes of Peach Sandstorm like the defense sector, activists, journalists, the list goes on (Microsoft Threat Intelligence, 2023). Like Peach Sandstorm PHOSPHOROUS is also sponsored by the Iranian Revolutionary Guard Corps (IRGC) and military. Back in 2023 around the same time that Peach Sandstorm was weaponizing CVE-2022-47966 in Zoho ManageEngine, PHOSPHOROUS was doing the same. Microsoft noted that the group is highly skilled in the rapid incorporation of different vulnerabilities into their tradecraft. The weaponization of ManageEngine shows that perfectly. The group’s attack pattern would also follow one of two ways. The first attack pattern, after gaining access through ManageEngine, would then proceed with the group then using Impacket to accomplish lateral movement to gain root access. In conjunction with that, the nation-state actor relied extensively on PowerShell scripts to locate admin accounts and turn on RDP connections. Impacket is an open-source framework for Python that allows working with networking protocols and concepts. PowerShell is essentially the Windows equivalent to the Linux terminal. RDP or Remote Desktop Protocol is a network protocol that is used for remote connections to different machines on a network. Obviously, attackers want to utilize this service so that one, if need be, they can maintain persistent remote access into their target’s infrastructure and, two, use RDP to connect to the target’s network and wreak the impending havoc that was intended. SSH or secure shell was used for connecting purposes so that they would immediately have the root access if anything. The end of the attack would end with the exfiltration of the target’s Active Directory database. With access to the database, the group could use the data, which was user account credentials, to login and pose as legitimate users (Microsoft Threat Intelligence, 2023). The second attack pattern would be done with Impacket but then followed by *Webhook.site* instead of RDP or SSH to maintain persistence and deploy malware such as Drokbk or Soldier. *Webhook.site* is an intermediary service that allows for the proxying of networking requests and the sending of actual webhooks to services that are placed behind a network’s firewall. *Webhook.site* would allow for the transformation of the information to different formats. Drokbk, although highly sophisticated, in simple terms searched for a directory on a target server or system and assisted with the transfer of data to another medium. Soldier is much similar.

To conclude, Iranian nation-state actors both Peach Sandstorm, PHOSPHOROUS and those alike will continue to get more and more sophisticated, and it is highly recommended that those who rely heavily on Azure services or any of the above services in this writing piece stay up to date with patches and harden their systems accordingly. Many cybersecurity professionals around the world would concur with the statement of, “It is not a matter of if you get hacked, but a matter of when you get hacked.” The security of your data, whatever kind it may be, should be at the forefront of your priorities and your networking or I.T. infrastructure should be taken seriously now, not later, if you are a business owner.

Sources

Intelligence, M. T. (2023, December 20). *Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

Team, N. T. R. (2024, April 12). *Analysis of FalseFont Backdoor used by Peach-Sandstorm Threat Actor*. Nextron Systems GmbH. https://www.nextron-systems.com/2024/01/29/analysis-of-falsefont-backdoor-used-by-peach-sandstorm-threat-actor/

Intelligence, M. T. (2023, October 18). *Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/

DrokBk malware uses GitHub as dead Drop resolver. (n.d.). Secureworks. https://www.secureworks.com/blog/drokbk-malware-uses-github-as-dead-drop-resolver

U.S. relations with Iran - United States Department of State. (2023, April 26). United States Department of State. https://www.state.gov/u-s-relations-with-iran/