OilRig Targets Technology Service Provider and Government Agency with QUADAGENT

Unit 42
Palo Alto Networks

Published on: August 14, 2018
Updated: August 16, 2018
Tags: Invoke-Obfuscation, OilRig, QUADAGENT, Threatlabz

The OilRig group continues to adapt their tactics and better their toolset with newly developed tools. The OilRig group UNA AKTSA, Helix Kitten is an adversary motivated by espionage primarily operating in the Middle East and Europe. Unit 42 has been tracking the OilRig group since 2015 and has documented several campaigns over that time frame. They have shown themselves to be an extremely persistent adversary that shows no sign of slowing down. Examining their past behaviors with current events only seems to indicate that the OilRig group's operations are in line with the interests of the Iranian government.

Between May and June 2018, Unit 42 observed multiple attacks by the OilRig group, assessed by us to originate from a government agency in the Middle East. Based on previously observed tactics, it is highly likely the OilRig group used spear phishing, watering hole and compromise attacks against the government agency as a launching platform for their true attacks.

The targets in these attacks included a technology service provider as well as another government entity. Both organizations are located in the Middle East. Based on the tools, tactics and infrastructure used, we believe they have originated from other entities in the same country. However, the actual attackers themselves were outside this country and likely used stolen credentials from the intermediary organization to carry out their attacks.

In this blog we will discuss the technical details of the attacks against the technology service provider. We will cover Invoke-Obfuscation Case Study and PowerSploit. In our own analysis, we were able to also confirm the attribution of this tool to the OilRig group by examining specific artifacts that were reused from tools previously used by the OilRig group. We will also discuss the technical details of the QUADAGENT tool. This tool is a multi-function malware technique used by the OilRig group as we have previously documented. However, packaging these scripts into a portable executable (PE) file is not a tactic we have seen the OilRig group use frequently. Detailed analysis of QUADAGENT is beyond the scope of this blog but we will provide a high level overview. QUADAGENT is the 2nd malware tool that Unit 42 has documented the OilRig group using for their attacks.

Our analysis revealed the two QUADAGENT PE files we obtained were slightly different from each other. Specifically, the variant that was used in the technology service provider attack was a .Net dll file, which can be seen in Figure 1. The other sample was a PE file generated as a DotNet tool.

SHA256	Filename	PowerShell Filename	Variant
1d1e1f2d8f7ddfc5144b8ec0f56ba5ccc9a7a5f7f4f0c3ec5ef9f8b8e4d3	CredentialProfile.exe	OfficeJsonDotNetCheck.exe	DotNet
2f8f8d9f7f5c6e7f8f6f7f9f7f9f8f8d9f7f5c6e7f8f6f7f9f7f9f8f8d9f	CallUtils.exe, Parser	SystemUtilsCleaner.ps1	.NET
7f8f9f7f5c6e7f8f6f7f9f7f9f8f8d9f7f5c6e7f8f6f7f9f7f9f8f8d9f	Microsoft.Net.Core.exe		

Table 1. QUADAGENT PE Files

The QUADAGENT backdoors dropped onto the hosts were nearly identical to each other, with the only differences being the command and control server (C2) and obfuscated obfuscation. We were also able to locate a third delivery package of the QUADAGENT backdoor as reported by ThreatLabz Cyber Security. In their example, the OilRig group used a Microsoft Word document to deliver the backdoor, which is a tactic much more commonly used by them.

A closer examination revealed the obfuscation used by the OilRig group in these QUADAGENT samples were similar to the tools they have used in previous attacks. Specifically, the OilRig group used Invoke-Obfuscation and deliverables in associating attributed PowerShell commands to better their deviance. Invoke-Obfuscation has proven to be highly effective at obfuscating PowerShell scripts and in this case, the adversary was able to take advantage of the tool for increased chances of evasion and as an anti-analysis tactic.

Attack Details

The OilRig group consisted of three waves between May and June 2018. All three waves involved a single spear phishing email that appeared to originate from a government entity based in the Middle East. Based on our telemetry, we have high confidence the email account used to launch this attack was compromised by the OilRig group prior to the attacks.

In the two waves (May 30 and June 2) against the technology services provider, the victim email addresses were not easily discoverable via common search engines, indicating the targets were likely part of a previously compromised email. The third wave against the government entity was compromised account used to send the attack emails. The malicious attachment was a simple PE file (SHA256: 5f1f1f2f8f7d6f1f1f4f6d6f1f5f6d6f1f1f4f6d6f1f5f6d6f1f1f4f6d6f) with the filename CredentialProfile.exe. This file was a .NET executable that was obfuscated using Invoke-Obfuscation. The file which will take batch files (.cmd and convert them to PE files. At one purpose-built backdoor, the QUADAGENT backdoor and execute it.

Once the victim downloads and executes the email attachment, it runs silently with no additional dialog elements or dialog boxes. The malicious attachment then drops the QUADAGENT backdoor into the %temp% folder and creates a .lnk file in the victim's startup folder to ensure persistence. The same Cleaner.lnk file will be used in the execution of it. A scheduled task is also generated to maintain persistence of the payload. Once the QUADAGENT payload has executed, it will use cmpgeoip.exe as the C2, that is HTTPS, then HTTP, then HTTP. Then the payload will use the following URL to check the connection to the C2 server:

The wave against the government entity (June 20) also involved a simple PE file (attachment SHA256: 4f6f6f6f7f5f6f6f6