OilRig APT Drills into Malware Innovation with Unique Backdoor

By Tara Seals

Published: 2020-07-22 · Archived: 2026-04-06 00:32:29 UTC

The RDAT tool uses email as a C2 channel, with attachments that hide data and commands inside images.

A series of cyberattacks on a telecom company in the Middle East has signaled the return of the OilRig APT. The attacks also revealed a revised backdoor tool in the group's arsenal, called RDAT.

The attacks were observed in April by Palo Alto Networks' Unit 42. Researchers there said that the version of RDAT in question was uncovered during the course of its investigation, standing out by using a unique command-and-control (C2) channel. To wit, it uses steganography to hide commands and data within bitmap images attached to emails.

The backdoor first debuted as a proprietary OilRig weapon in 2017 and has gone through several updates since then, the firm noted, adding that timestamps indicate that OilRig added the steganography trick to RDAT's profile as far back as 2018.

"In June 2018, the developer of RDAT added the ability to use Exchange Web Services (EWS) to send and receive emails for C2 communications," according to Unit 42's report, issued Wednesday. "This email-based C2 channel is novel in its design, as it relies on steganography to hide commands and exfiltrates data within BMP images attached to the emails. The combination of using emails with steganographic images to carry the data across the C2 can result in this activity being much more difficult to detect and allow for higher chances of defense evasion."

Along with RDAT, OilRig in the telecom campaign used custom Mimikatz tools for collecting credentials, Bitvise to create SSH tunnels and PowerShell downloaders to perform post-exploitation activities.

"Two of the related tools collected had PDB paths similar to ones we had seen in the past. The PDB paths were C:\Users\Void\Desktop\dns\client\x64\Release\client.pdb and C:\Users\Void\Desktop\RDAT\client\x64\Release\client.pdb," according to Unit 42. "Using the file path of the user in the PDB string of C:\Users\Void\Desktop as shown in Figure 1, we gathered over a dozen samples with that file path, with most of the samples identified as a known OilRig tool called ISMDOOR. Considering the small cluster of related tools, it is highly likely these have been developed by a single adversary or adversary group with control over the codebase."

In May, Symantec published research on the Greenbug group targeting telecommunications organizations in Southeast Asia. Unit 42 has previously linked Greenbug to OilRig, a threat group that first emerged in 2015.

The Novel C2 Channel

RDAT communicates with two hardcoded actor-controlled email addresses: koko@acrlee[.]com and h76y@acrlee[.]com. It simply sends email to the actor-controlled email addresses, attaching Bitmap images that contain hidden messages or data to exfiltrate.

“To send emails from the compromised host, the payload uses the email associated with the account logged into the compromised host, as it uses the WinHTTP library to make requests to the API [with the security level in the auto-login policy field set to low], which automatically attempts to log onto Exchange using the default credentials,” according to the report.

OilRig meanwhile communicates with RDAT in turn by sending emails to the compromised account. RDAT creates an inbox rule to move any incoming C2 messages t the junk folder, then continually looks there for commands, which are hidden within Bitmap images.

“The payload will issue a request to the EWS API to check for unread emails from the actor’s email addresses with an attachment,” researchers said. “If the payload obtains an email sent by the actor, the payload will process the response to the SOAP request and send additional requests to the EWS API to get the email, the attachment and the contents of the attachment…It then saves this content to a file in the %TEMP% folder with a ‘.bmp’ file extension. It then issues a SOAP request to delete the processed email.”

The email C2 channel supplements the HTTP and DNS-tunneling C2 channels seen in other RDAT samples, researchers said. But regardless of the C2 channel used, the RDAT sample parses responses using a command handler to determine the course of action to take. These include the ability to execute commands, upload and download to and from the C2, take screenshots, restart its processes and delete itself.

“The majority of samples used some combination of HTTP and DNS tunneling channels, with the single exception where we discovered the developer leveraging Exchange Web Services to send and receive emails to and from the actor using steganographic image file attachments,” the report concluded. “The use of a novel C2 channel in combination with steganography shows the continued evolution and development of different tactics and techniques by this adversary over time.”

OilRig Continues Its Activity

Believed to be a state-sponsored group under the auspices of to the Iranian intelligence agency and the Islamic Revolutionary Guard Corps (IRGC), OilRig’s primary purpose appears to be espionage efforts targeted at financial, aviation, infrastructure, government and university organizations in the MidEast region.

It’s known for continually evolving its tools. The group, which is also called Cobalt Gypsy, Crambus, Helix Kitten or APT34, for instance was seen in February establishing a highly developed and persistent infrastructure that could be converted to distribute destructive wiper malware. That malware, known as ZeroCleare, was spotted in December.

Source: https://threatpost.com/oilrig-apt-unique-backdoor/157646/