OilRig Deploys “ALMA Communicator” – DNS Tunneling Trojan

researchcenter.paloaltonetworks.com/2017/11/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

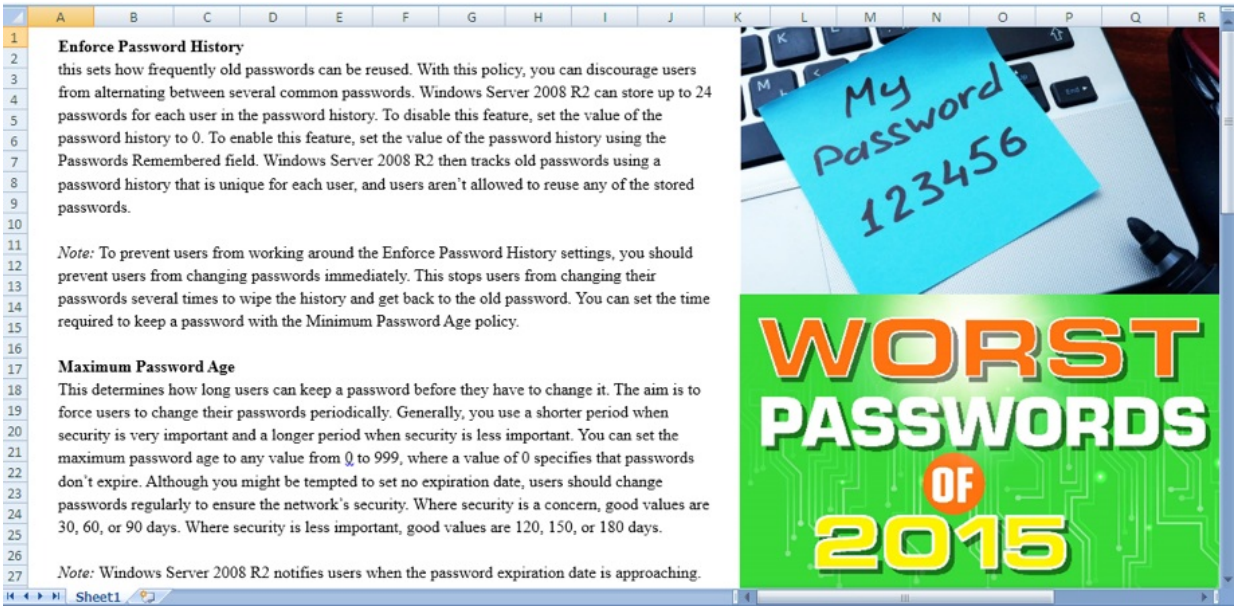
By Robert Falcone November 8, 2017

Unit 42 has been closely tracking the OilRig threat group since May 2016. One technique we’ve been tracking with this threat group is their use of the Clayslide delivery document as attachments to spear-phishing emails in attacks since May 2016. In our April 2017 posting OilRig Actors Provide a Glimpse into Development and Testing Efforts we showed how we observed the OilRig threat group developing and refining these Clayside delivery documents.

Recently, we observed a new version of the Clayslide delivery document used to install a new custom Trojan whose developer calls it “ALMA Communicator”. The delivery document also saved the post-exploitation credential harvesting tool known as Mimikatz, which we believe the threat actors will use to gather account credentials from the compromised system. While we do not have detailed telemetry, we have reason to believe this attack targeted an individual at a public utilities company in the Middle East.

New Clayslide Delivery Document

The most recent build of Clayslide operates in a similar way to its predecessors, as it initially displays an “Incompatible” worksheet that states that the Excel file was created with a newer version of Excel and the user needs to “Enable Content” to view the document. If the user clicks “Enable Content”, a malicious macro will run that begins by displaying a hidden worksheet that contains decoy contents, as seen in the following:



While the decoy is displayed to the victim, the malicious macro accesses data from specific

cells in the “Incompatible” worksheet that it concatenates to create an .HTA file, which it then saves to %PUBLIC%\tmp.hta and opens with the mshta.exe application. The .HTA file contains HTML that will run a VBScript that finally installs the malicious payload for this attack.

The payload installation process begins with the .HTA file creating a folder named %PUBLIC%\{5468973-4973-50726F6A656374-414C4D412E-2}, to which it writes three files with the following names:

- SystemSyncs.exe
- m6.e
- cfg

The .HTA file contains two encoded executables that it will decode and write to m6.e and SystemSyncs.exe. The .HTA file contains a base64 encoded configuration that it decodes and saves to the cfg file, which the Trojan will use to obtain the C2 domain that it will use to communicate with the threat actor. The C2 domain saved to the cfg file in this attack is prosalar[.]com.

The SystemSyncs.exe file (SHA256: 2fc7810a316863a5a5076bf3078ac6fad246bc8773a5fb835e0993609e5bb62e) is a custom Trojan created by the OilRig group called “ALMA Communicator”, which we will describe in detail in the next section.

The “m6.e” file dropped by the .HTA file is a variant of Mimikatz (SHA256: 2d6f06d8ee0da16d2335f26eb18cd1f620c4db3e880efa6a5999eff53b12415c) tool. We have seen the OilRig threat group using Mimikatz for credential gathering during its post-exploitation activities, however, this is the first time we have observed the threat group delivering Mimikatz during the delivery phase of the attack. We believe the Clayslide delivery document dropped this additional tool based on the limitations of ALMA Communicator’s C2 channel, which we will describe later in this report.

The VBScript in the .HTA file executes the SystemSyncs.exe payload and achieves persistent execution by creating a scheduled task. Unlike past Clayslide documents that create a scheduled task via the schtask application via the command prompt, the VBScript programmatically creates the task using the Schedule.Service object. The scheduled task created, as seen in Figure 1, shows that the payload will be executed every two minutes with the command line argument “Lock”.

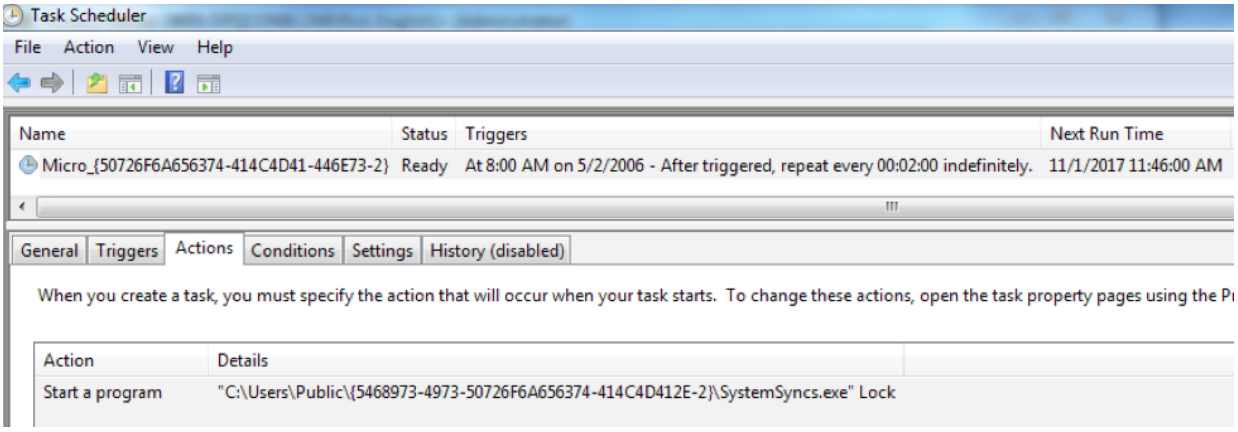


Figure 1 Scheduled task created by Clayslide to execute the ALMA Communicator payload

ALMA Communicator Trojan

The ALMA Communicator Trojan is a backdoor Trojan that uses DNS tunneling exclusively to receive commands from the adversary and to exfiltrate data. This Trojan specifically reads in a configuration from the cfg file that was initially created by the Clayslide delivery document. ALMA does not have an internal configuration, so the Trojan does not function without the cfg file created by the delivery document.

After reading in its configuration, the Trojan creates two folders for staging, named Download and Upload. ALMA uses the Download folder to save batch files provided by the C2 server, which it will eventually run. ALMA uses the Upload folder to store the output of the executed batch files, which it will eventually exfiltrate to the C2 server.

ALMA Communicator uses DNS tunneling as its C2 communication channel using a specific protocol that uses specially crafted subdomains to transmit data to the C2 server and specific IPv4 addresses to transmit data from the C2 to the Trojan. The transmission of information from the Trojan to the C2 server occurs through DNS requests to resolve specially crafted subdomains on the configured C2 domain.

To build these specially crafted subdomains, the Trojan generates a random four-digit number and concatenates a hardcoded string of ID. The Trojan then appends a unique identifier for the compromised system to this string. To generate this unique identifier, the Trojan starts by obtaining the system's ProductId from the registry, specifically at SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductId. If it cannot find this registry key, it will use the hardcoded value 00000-00000-00000-00000. It then obtains the username and concatenates an underscore followed by the product id string. The Trojan takes the MD5 hash of this string and uses it as the basis for the unique identifier for the compromised system. It then appends the hardcoded -0-2D-2D string to finish the construction of the subdomain used to beacon the C2 server. Figure 2 shows the structure of the domains that ALMA communicator will send to the C2 server to receive data.

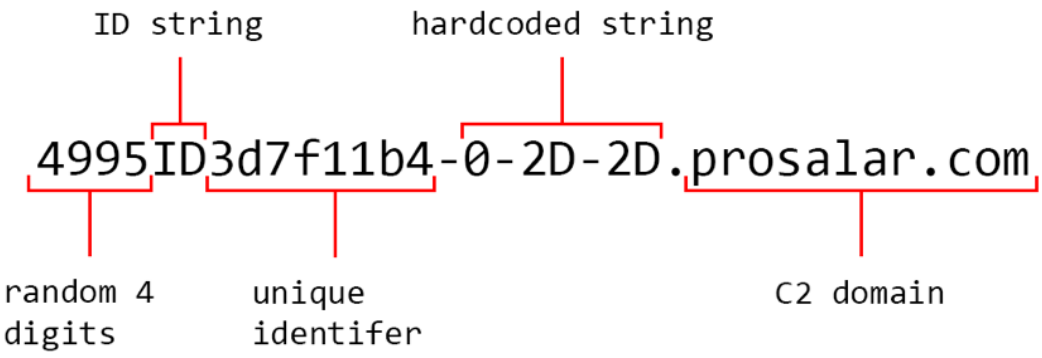


Figure 2 Domain used by ALMA communicator to receive data from the C2 server

To provide a better explanation of the unique identifier generated by ALMA communication, let's consider a test system with the username and product id create the string Administrator_00000-00000-00000-00000, which results in an MD5 hash of 35ead98470edf86a1c5a1c5fb2f14e02. The Trojan will generate the unique identifier string 3d7f11b4 by taking the first, fifth, ninth, thirteenth, seventeenth, twenty first, twenty fifth and twenty ninth characters from the MD5 hash and concatenating them together, as seen in Figure 3.

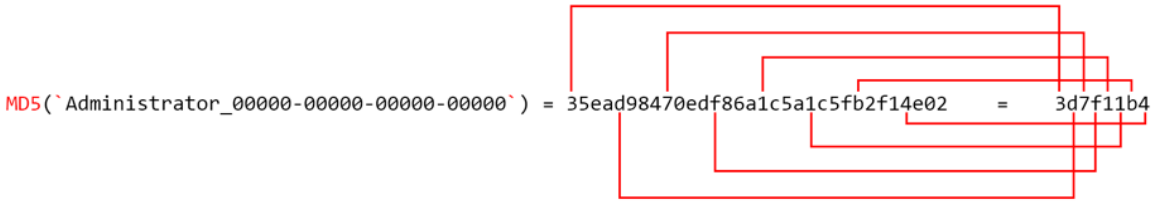


Figure 3 How ALMA Communicator generates the unique identifier for the compromised system

The C2 server will reply to the beacon DNS requests with IPv4 addresses within A records. The Trojan will parse these requests for two specific IP addresses, one to mark the beginning and one to mark the end of the transmission of data from the C2 to the Trojan. The two specific IP addresses to mark the start and end of the data are:

Start – 36.37.94.33 ($%^!)

End – 33.33.94.94 (!!^^)

The C2 will respond to DNS queries between these two responses with IP addresses that the Trojan will treat as binary data. During our analysis, we observed the following data being sent from the C2 server to our analysis system, with $%^! and !!^^ representing the start and stop markers for the data:

```
$%^!_DnsInit.bat@echo off & chcp 65001\r\necho
%userdomain%\\%username% 2>&1 & echo %computername% 2>&1 & echo

_____Task_____
& schtasks /query /FO List /TN "Google_{50726F6A656374-
414C4D41-48747470}" /V | findstr /b /n /c:"Repeat: Every:" 2>&1
& schtasks /query /FO List /TN "Micro_{50726F6A656374-
414C4D41-446E73-2}" /V | findstr /b /n /c:"Repeat: Every:" 2>&1 & echo
_____ !!^^
```

Based on the data sent back from the C2, the Trojan will create a file named _DnsInit.bat with commands seen in the data. The Trojan stores the batch file in the Download folder. The Trojan will then enumerate this folder and create a cmd.exe process with the path to the batch script as a command line argument. The Trojan will add to the command line argument the string " > " followed by the batch script's filename with the .txt.Prc file extension to write the output of the command to a text file in the Upload folder. Before running the process, the following string to the end command line argument to delete the batch script upon execution:

\r\nDEL /f /q \"%~0\"|exit

The Trojan will then attempt to send the newly created file in the Upload folder that contains the result of running the command. The DNS requests used to send this data has four fields that are split up using a hyphen, which are:

1. Random four-digit number followed by static "ID" string and the 10 character unique system identifier
2. Number of DNS queries needed to send entire data stream
3. Maximum of 20 characters for 10 hexadecimal bytes of data to transmit
4. String of characters for hexadecimal bytes for filename transmitted

To better visualize the structure of a DNS query used to send data, the following is shows the domain name that the Trojan will build to send data to its C2 server:

[random 4 digits]ID[unique identifier]-[number of DNS queries needed]-[string of hexadecimal bytes for sent data]-[string of hexadecimal bytes for filename being sent].prosalar[.]com

For example, figure 4 is the first DNS query issued after our testing system ran the _DnsInit.bat script provided by the C2 server mentioned above. As you can see, each DNS request can only send 10 bytes of data at a time, requiring 29 outbound requests to transmit the 289 bytes of output that was generated by the batch script.

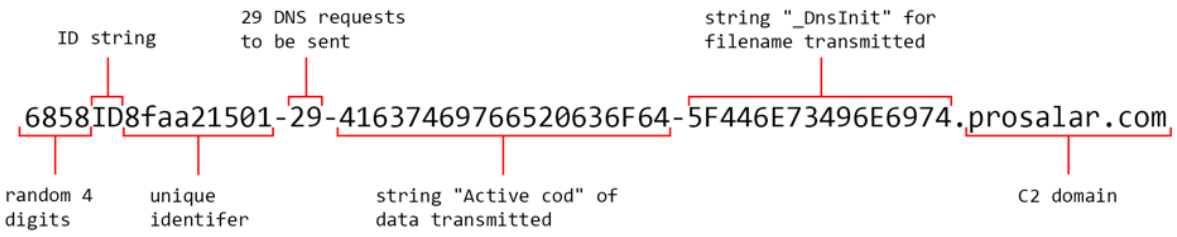


Figure 4 Subdomain that ALMA Communicator attempts to resolve to transmit data to its C2 server

As you can surmise, ALMA Communicator's C2 channel is rather limited when it comes to data transfer. If an actor wished to use ALMA communicator to exfiltrate large files, it would result in a very large number of outbound DNS requests, as each outbound request can only send 10 bytes at a time. Even more limiting is the data transmission from the C2 server to the Trojan, which can only send 4 bytes per DNS request, as each IPv4 address is treated as data. We believe this is the reason why the Clayslide delivery document saved the Mimikatz tool to the system instead of having the actor download the tool to the system after a successful compromise. Based on the 4-byte per DNS request limitation, the ALMA Communicator would generate 189,568 DNS requests (not including the start and stop requests) to transmit the 758,272 byte Mimikatz tool to the system, which may be detected by security systems or personnel.

Conclusion

The OilRig threat group continues to use their Clayslide delivery document in their attack campaigns. The current variant of Clayslide also suggests that this group continues to develop these delivery documents with new installation techniques to evade detection. This threat group also continues to add new payloads to their toolset as well, with ALMA Communicator being the most recent addition. Lastly, it appears that OilRig still prefers using DNS tunneling for its C2 channel of choice, as ALMA Communicator, Helminth and ISMAgent all use this technique for C2 communications.

Palo Alto Networks customers are protected by the following:

- WildFire identifies ClaySlide delivery documents and ALMA Communicator samples as malicious
- Traps blocks the ALMA Communicator Trojan via Local Analysis and blocks the Clayslide delivery document based on "Suspicious macro detected"
- AutoFocus customers can track these tools using the following tags:
    - Clayslide
    - ALMACommunicator
    - Mimikatz

Indicators of Compromise

f37b1bbf5a07759f10e0298b861b354cee13f325bc76fbddfaacd1ea7505e111 (Clayslide)

2fc7810a316863a5a5076bf3078ac6fad246bc8773a5fb835e0993609e5bb62e (ALMA Communicator)

2d6f06d8ee0da16d2335f26eb18cd1f620c4db3e880efa6a5999eff53b12415c (Mimikatz)

prosalar[.]com