

Tunneling Under the Sands

By ASERT team

Published: 2018-09-14 · Archived: 2026-04-06 00:10:13 UTC

Executive Summary

ASERT recently came across spear-phishing emails targeting the Office of the First Deputy Prime Minister of Bahrain. A similar campaign uncovered by Palo Alto's [Unit 42](#) found the activity distributing an updated variant of [BONDUPDATER](#), a PowerShell-based Trojan, which they attribute to Iranian APT group OilRig (aka APT34). ASERT was able to uncover Command and Control (C2) traffic instructing the script to run commands, including the C2 responses from the attacker's server. **NOTE:** *Netscout APS enterprise security products detect and block all network IOCs noted in this report.*

Key Findings

- BONDUPDATER, a PowerShell based Trojan, now obfuscates the data prior to exfiltration.
- Data exfiltration occurs using inserted sub-domains for each communication to the attacker's C2 server.

Analysis

During the course of ASERT's investigation into the alleged Oilrig activity, we managed to capture live C2 communications, and reverse engineer the communication protocols the malware uses. For further details on the malware itself and how it behaves, we recommend reading the blog that Unit42 [security researchers](#) published earlier in the week. The BONDUPDATER C2 communications utilize DNS queries for communication and data exfiltration. Specifically, BONDUPDATER uses DNS A records and DNS TXT records to relay the information.

Command Delivery

BONDUPDATER makes use of the TXT data field to pass commands to the client. DNS TXT records are traditionally used to provide additional information about the domain; however, it could be anything, provided it follows the standard. Here, the attacker abuses the functionality to deliver items like commands. The command format the attackers send in the TXT response field is: *5 characters > Data* (Figure 1).

TXT: S0000>d2hvYW1pJm1wY29uZm1nIC9hbGw=

Figure 1: S0000 Command

The script splits the command into two parts delimited by the > character. For example, to run a simple command on the victim machine, the attacker would respond to three separate DNS TXT queries with the following responses:

1. S000s>10100
 1. Create a file under the receivedbox folder called rcvd10100
2. S0000>d2hvYW1pJm1wY29uZm1nIC9hbGw=
 1. Decode command to the right of >
 1. Replace('-', '+')
 2. Replace('_', '/')
 3. Base64 Decode
3. E0000>0
 1. Write the decoded command to the file

Data Exfiltration

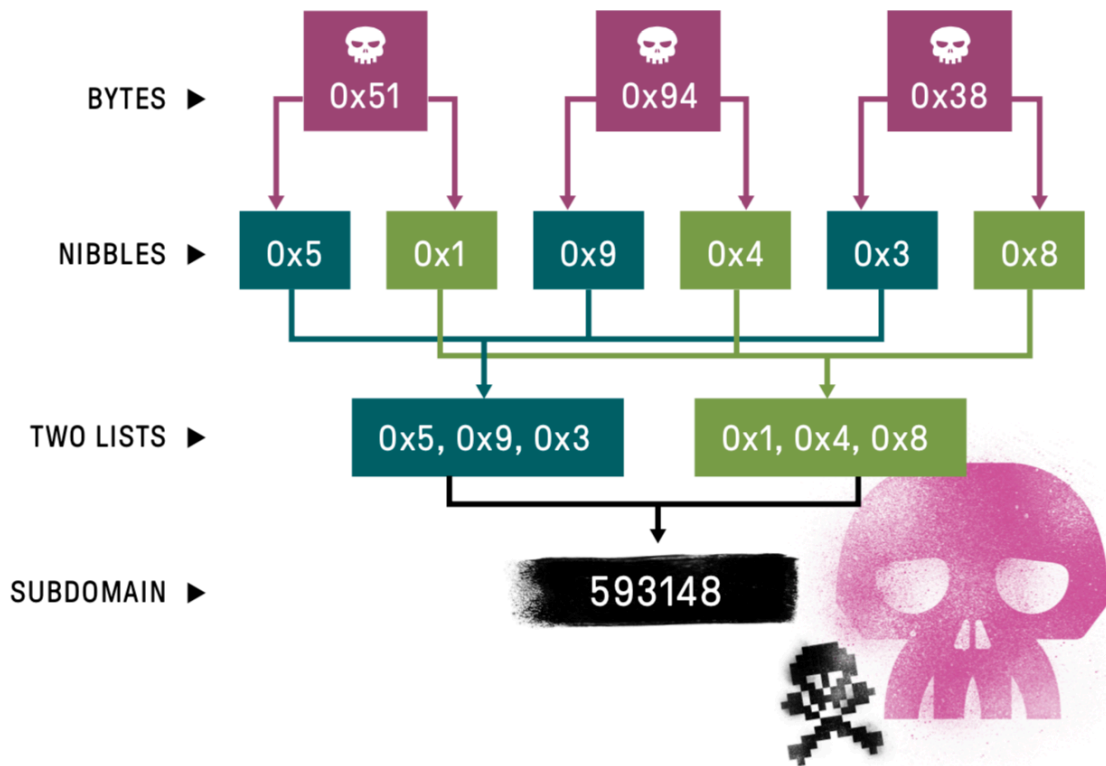


Figure 3: Binary Scrambling

The script below reorganizes the nibbles into their respective bytes (Figure 4).

```
import binascii
data = 'EBB466767667256666772556776662FBFD932F3F64079E4F730B65239FE0'
exfil_data = []
for x in range(int(len(data)/2)):
    try:
        exfil_data.append(binascii.unhexlify(data[x] + data[int(len(data)/2)+x]))
    except:
        exfil_data.append(data[x] + data[int(len(data)/2)+x])
print(''.join(exfil_data))
```

Figure 4: Python2 snippet to reconstruct the data

The above code snippet returns: *Microsoft Windows [Version, which is part of the output when running the following command:*

- whoami&ipconfig /all

Command Identification Marker

The third level subdomain contains an identification marker as noted below:

- <redacted>.COCTabCOCT.33333210100A[.]withyourface[.]com

The value equals the command identifier specified by the S000s command (above). Similar to a campaign ID/name, it is likely the attackers use this marker to categorize and sort C2 communications. This subdomain also uses the same algorithm defined in Figure 3.

Summary & Recommendations

APT actors continually revamp and develop new capabilities to add to their portfolio and BONDUPDATER is no exception. The custom DNS tunneling and obfuscation technique allows the attacker to circumvent some defense measures. From a defender's perspective, ASERT recommends that all DNS traffic be monitored for abnormal behavior such as abnormally long domain names. At a minimum, inspect DNS A records for "COCTab" which could be a sign of this specific infection. Practice good email hygiene and disable scripts from running in Office documents where possible. Enable PowerShell logging to monitor for suspicious behavior. Research into this group and specifically BONDUPDATER, reveals that the actor is continuously improving their toolset to maximize their chances of success. Thus, layered controls are essential for detecting the threats of tomorrow.

IOCs

- [withyourface\[.\]com](https://withyourface.com)
- 52b6e1ef0d079f4c2572705156365c06 - Word Document
- 8c4fa86dcc2fd00933b70cbf239f0636 - PowerShell Script

Source: <https://www.netscout.com/blog/asert/tunneling-under-sands>