Striking Oil: A Closer Look at Adversary Infrastructure

By Robert Falcone, Bryan Lee

Published: 2017-09-26 · Archived: 2026-04-05 16:59:08 UTC

While expanding our research into the TwoFace webshell from this past July, we were able to uncover several IP addresses that logged in and directly interfaced with the shell we discovered and wrote about. Investigating deeper into these potential adversary IPs revealed a much larger infrastructure used to execute the attacks. We found the infrastructure was segregated into different functions for specific malicious objectives. We found some sites that were set up as credential harvesters (likely used in phishing attacks), a compromised system that was used to interact with a TwoFace webshell to hide the actor's location, and finally systems that interact with TwoFace webshell-compromised systems to provide command and control direction of those compromised systems.

In addition to uncovering the attack infrastructure for this adversary, we were able to determine a significant link between the operators of the set of attacks involving TwoFace and another attack campaign we have published on in detail: OilRig.

Spoofing Sites and Credential Harvesters

We observed the IP address 137.74.131[.]208 interacting with the TwoFace webshell as described in our previous blog. Our investigation of the passive DNS entries for this IP revealed a potential link to a credential harvesting campaign carried out by the threat group behind the TwoFace webshell attacks. Looking into passive DNS entries for the IP gave us the following domain resolutions:

- owa-insss-org-ill-owa-authen[.]ml
- webmaiil-tau-ac-il[.]ml
- mail-macroadvisorypartners[.]ml
- webmail-tidhar-co-il[.]ml
- my-mailcoil[.]ml
- logn-micrsftonine-con[.]ml
- so-cc-hujii-ac-il[.]ml

These domain names, on initial inspection, appear to be emulating legitimate webmail login portals, indicating that these are likely to be credential harvesters. We confirmed this as seen below:

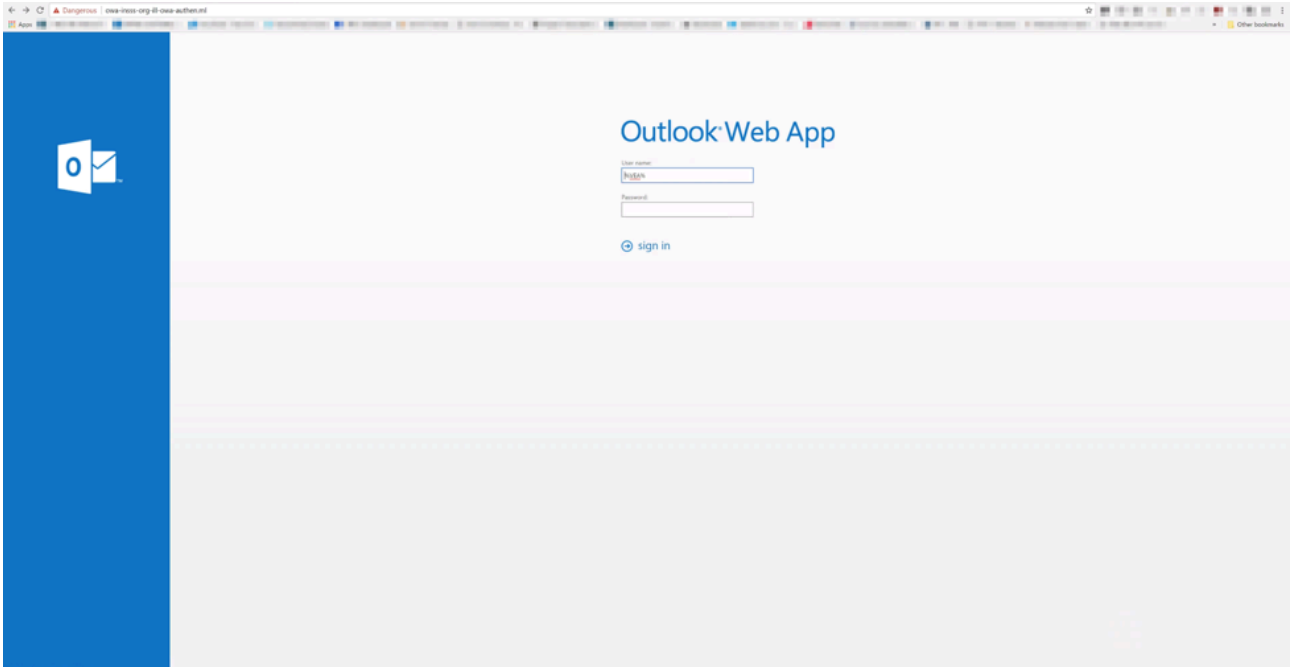

Figure 1a. Example of a credential harvester

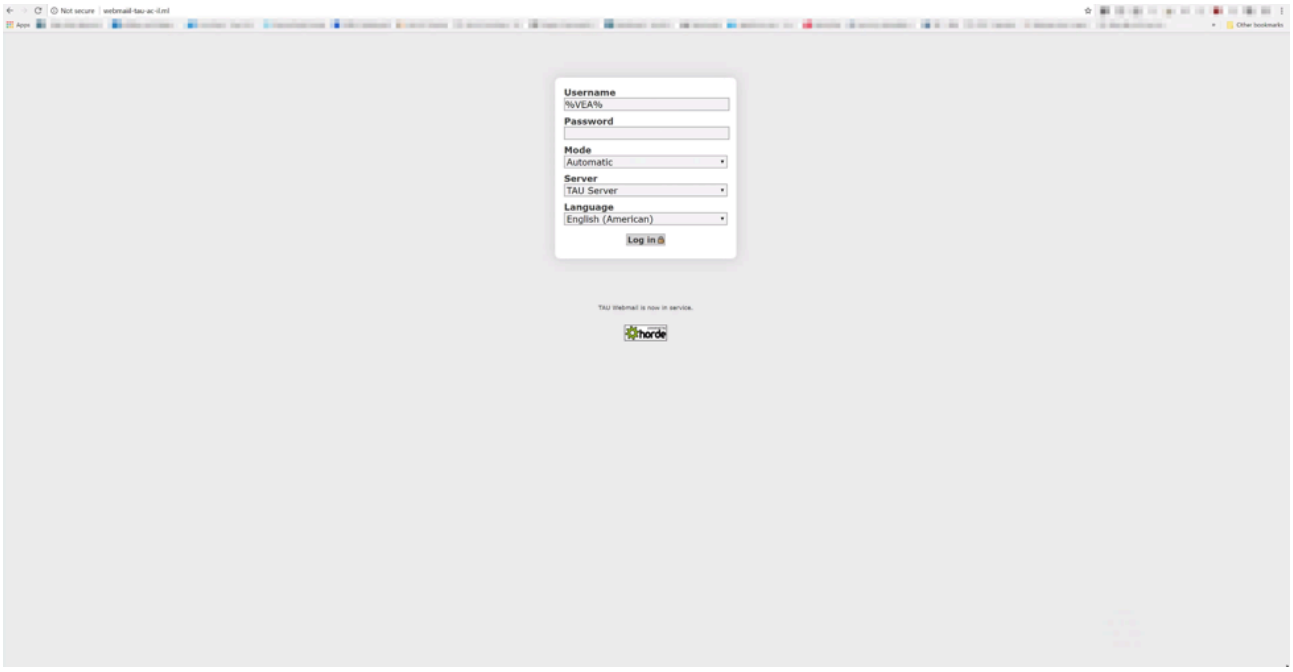

Figure 1 b. Example of a credential harvester

Our further examination revealed that these credential harvesters were crafted to be exact replicas of the legitimate sites they were purporting to be. This is a common tactic deployed by adversaries leveraging credential harvesters to increase the chance that a user will input their credentials and decrease suspicion of nefarious activity.

Breaking down the intended targeting for these credential harvesters reveals interesting target grouping.

- owa-insss-org-ill-owa-authen[.]ml is likely intended to mimic the INSSS or the Institute of National Security Studies, a thinktank for Israel's national security agenda.

- webmaiil-tau-ac-il[.]ml is likely intended to mimic Tel Aviv University, the largest university in Israel.
- mail-macroadvisorypartners[.]ml is likely intended to mimic Macro Advisory Partners, a prominent strategic consulting firm that has published insights into the Israel region.
- webmail-tidhar-co-il[.]ml is likely intended to mimic the Tidhar Group, an Israeli based real estate and property management company.
- my-mailcoil[.]ml is likely intended to mimic Bezeq International's webmail application. Bezeq International is an Israeli based telecommunications company providing consumer and enterprise services.
- so-cc-hujii-ac-il[.]ml is likely intended to mimic the Hebrew University of Jerusalem which is the second oldest university in Israel.

Each of these organizations appear to be either Israeli based or have strong Israeli connections and interests. Credential harvesters in general are not uncommon, but it is significant to have a grouping of region and company specific harvesters. This grouping leads us to believe that this adversary is likely to have had a specific mission to accomplish, which involved breaching specific organizations. This is in contrast to more generic credential harvesting by targeting common applications such as Gmail or Facebook.

The relationship between the credential harvesters hosted on 137.74.131[.]208 and the interaction with TwoFace is still unclear at this time. We do know the operator of TwoFace had access to both TwoFace and these spoofing sites. And it is highly unlikely that it is a coincidence that these specifically designed spoofing sites were on the same infrastructure as TwoFace when both target the same geopolitical region.

Additional Webshells

By analyzing additional TwoFace samples, as well as the traffic seen associated with TwoFace, we were able to find additional webshells used by this threat group. The additional webshells show that this threat group does not solely rely on TwoFace when deploying a webshell on a compromised web server.

RunningBee

A second IP of high interest seen interacting with the TwoFace webshell was 192.155.x.x, which is owned by SoftLayer. This IP resolves to a domain owned by the Ministry of Oil of a nation-state in the Middle East. The use of this IP is interesting as there are only two possibilities as to why this specific IP would be directly interfacing with the TwoFace shell: either it is the adversary themselves, or it has been compromised and is being used as part of the adversary infrastructure.

Based upon additional telemetry found in AutoFocus, we believe it is highly likely that this IP was indeed compromised and added to the adversary infrastructure. The telemetry revealed that this IP was not only used to interact directly with the TwoFace shell discussed in our previous blog, but also used to upload post-exploitation tools to another shell hosted on a Middle Eastern educational institution. We have named this second webshell "RunningBee".

RunningBee is a webshell that requires an actor to enter a password before running commands or uploading files to the webserver much like TwoFace. However, the shell itself is different from a UI and code perspective. The samples of RunningBee that we identified requires the password "NeshaNesha12" for interaction. This is notable

because this same password was mentioned in Cylance's Operation Cleaver report as a password for webshells used by one of the members of that operation.

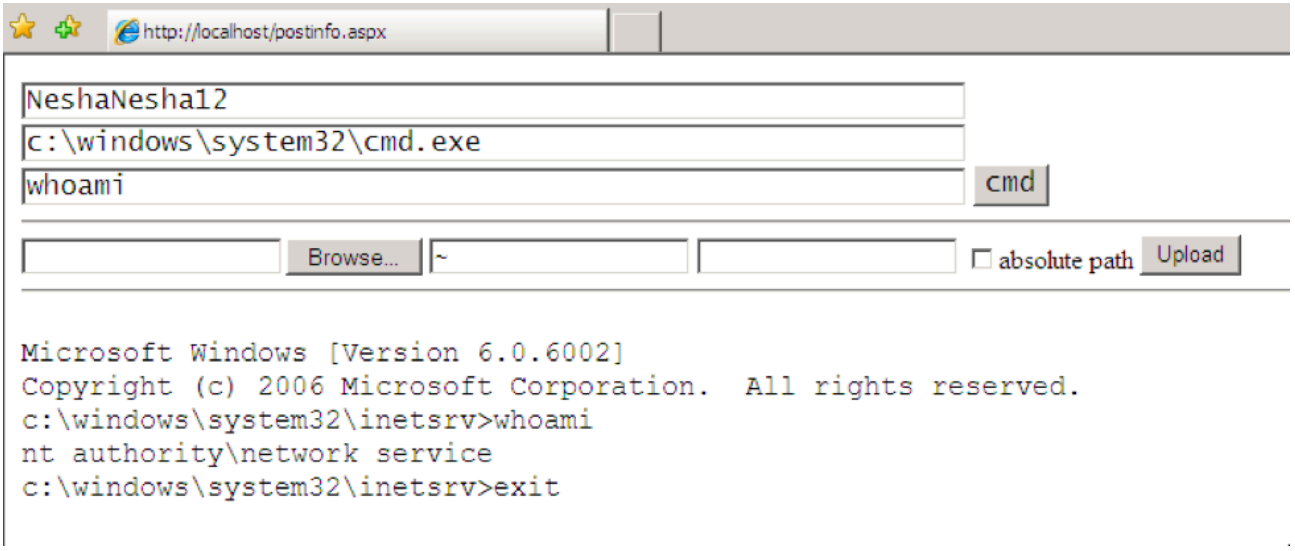

Figure 2 RunningBee webshell

Investigating RunningBee activity revealed that the 192.155.x.x IP uploaded at least four additional tools to that compromised system with RunningBee on it, as seen in Table 1. Please reference the 'Post-exploitation Tools SHA256' section at the end of this blog for full hashes of the tools mentioned throughout in this blog.

Date Uploaded	SHA256	Filenames	Tool
10/06/2016, 02/19/2017	3b08535b4add194...	PsExec.exe, kb-11.exe	PsExec
02/19/2017	28a0db561ff5a52...	kb.exe	Mimikatz
02/19/2017	450ebd66ba67bb4...	Local.exe	Local.Exe of Microsoft Windows NT Resource Kit
02/19/2017	5b7eb534a852c18...	kbs.exe	Mimikatz

Table 1 Post-exploitation tools found on RunningBee

The uploaded files were common examples of tools often found during the post-exploitation phase.

- Psexec – a lightweight application part of the SysInternals package designed to execute processes on other systems and allow for interactive console access
- Mimikatz – an open source tool designed to extract and use credential information from Windows systems
- local.exe – a command line tool part of the NT Resource Kit to view members of local groups on remote servers or domains

Our analysis showed the specific hashes of these tools were placed on multiple other sites also containing TwoFace related webshells, leading us to believe that they are related to one specific adversary.

Based on the post-exploitation tools uploaded to RunningBee and common IP addresses interacting with the shells, we found four other related webshells hosted on webservers belonging to organizations in the Middle East. The tools listed in Table 2 include the same tools that were uploaded to RunningBee such as PsExec, Mimikatz and Local.exe. In addition to these tools, we also discovered the existence of the remote connection tool known as PuTTY Link (plink) and a custom Microsoft IIS (Internet Information Services) web server backdoor that we track as RGDoor. We believe the threat actors may have used plink to connect to additional systems on the compromised network after obtaining legitimate credentials using a tool such as mimikatz. RGDoor is an HTTP module that the threat actors are likely loading into the IIS web server to maintain an additional, backup access point should the compromised organization detect and remediate the installed webshell (e.g. TwoFace, RunningBee) from the server.

SHA256	Filename	Tool	Shells	IP addresses uploading
744e0ce108598aa...	S64.exe		1	138.201.209.162
bb9b4e088eb9910...	z64.exe		1	89.163.206.0
28a0db561ff5a52...	mom64.exe	Mimikatz	2	137.74.131.208
6e623311768f1c4...	s64.exe		3, 4	51.254.50.153, 212.16.80.102, 37.59.229.231, 91.121.237.227
3b08535b4add194...	ps.exe	PsExec	3, 4	51.254.50.153
6ae32cd3b5a8a1d...	pl.exe	PuTTY Link	3, 4	51.254.50.153, 91.121.237.227, 37.59.229.231, 176.9.164.252
450ebd66ba67bb4...	Local.exe	Local.Exe of Microsoft Windows NT Resource Kit	3	91.121.237.227
d3b03c0da854102...	O6.exe	Mimikatz	1	92.222.209.48, 94.23.172.49
5ead94f12c30743...	O64.exe	Mimikatz	1	92.222.209.51
caf5f9791ab3049...	i64.exe		1	138.201.209.182, 5.39.59.97, 91.121.237.224
497e6965120a7ca...	HTTPParser.dll	RGDoor	1	5.39.59.97

Table 2 Post-exploitation tools and associated IPs

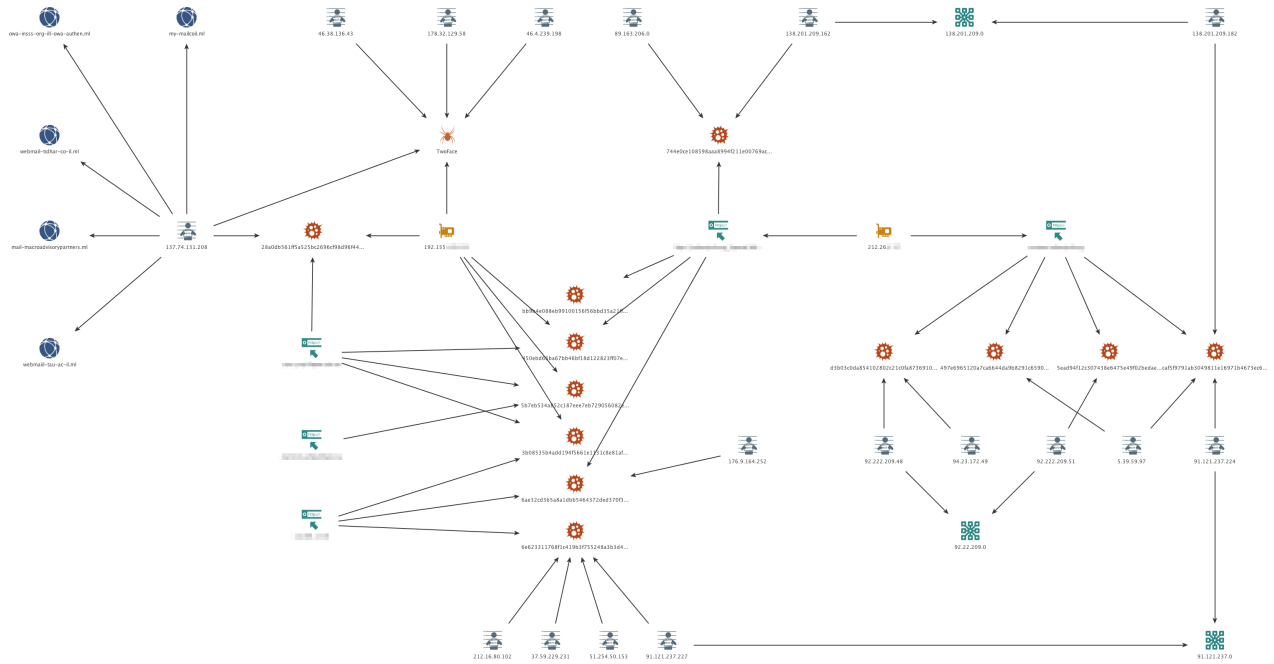

Figure 3 Visualization of relationships of webshell and tools

LittleFace

As we reported in our TwoFace blog, the TwoFace shell was unique in that it was actually two webshells, where after initial authentication to a loader webshell, a secondary webshell with additional functionality was unpacked and made accessible to the operator. After gathering additional TwoFace loader shells, we noticed that some of these TwoFace loaders contained an embedded shell that differed from the TwoFace payload we originally found and published in our previous blog. This different shell, which we call LittleFace, contains much less functionality and is relatively simple compared to its TwoFace payload counterpart. LittleFace also differs from the previous TwoFace payloads as once it is saved to the system, it no longer requires authentication.

The LittleFace shell does not display a web-based user interface like most webshells. Instead, it is a webshell that allows the threat actor to pass commands to Windows command prompt by issuing HTTP POST requests with the desired command within the “c” field of the posted data, as seen in the following code block that is the command handler on the webshell. The webshell will receive the commands embedded in the HTTP POST requests and hand them off to another function (“r” function in the following code block) for processing.

```
void Page_Load(object sender, EventArgs e)
{
    try
    {
        string cmd = Request["c"];
```

```
        r(cmd);
    }
    catch (Exception)
    {
    }
}
```

The LittleFace shell will execute the command ('r' function seen in code block above) by creating a "cmd.exe" process and writing the desired command to the process' standard input. The result of the command is provided back to the actor directly within the HTTP response to the POST request.

OilRig Link

While examining each of the tools that were found on the compromised sites, one specific sample of Mimikatz showed evidence of a potential relationship with the OilRig campaign.

As detailed in our April 2017 blog "OilRig Actors Provide a Glimpse into Development and Testing Efforts", we were able to track an entity that appeared to be testing and iterating through different variations and versions of tools associated with the OilRig campaign. This same entity was found submitting a specific sample of Mimikatz a day after testing multiple Helminth samples. We observed actors uploading this specific sample of Mimikatz to the TwoFace webshell hosted at the Saudi education institution mentioned earlier in this blog, leading us to believe that there is a likely relationship between the OilRig campaign and the TwoFace campaign. The extent of this relationship is unknown at this time. While we cannot be absolutely certain that this is the same adversary in both attacks, we are able to ascertain that this specific entity does have access to OilRig tools and also has access to a very specific sample of Mimikatz only found in this attack infrastructure.

Expanding on the possible relationship between TwoFace and OilRig, examining the tactical overlap of both attacks may also provide additional data points to link them. Specifically, significant targeting overlap exists with both attacks, with multiple organizations in multiple nation states throughout the Middle East region being targeted either as a final target or added as part of the attack infrastructure. One possible scenario of how TwoFace and OilRig are used in conjunction could be where the adversary uses the ClaySlide documents to deliver Helminth, which is then used as an initial landing point or beachhead into the target's network. From there, the adversary may use the initial ingress point and its corresponding permissions to install the TwoFace webshell on accessible systems. Additional post-exploitation tools such as the ones we discovered may then have been uploaded to the now compromised systems via the TwoFace file upload function.

Conclusion

As we have continued our research into operations in the Middle East, we are beginning to uncover more and more overlaps between the various adversary groups and campaigns outlined by us and others in the public

domain. In this incident, we were able to follow a trail starting from a single webshell to a bevy of compromised sites, credential harvesters, post-exploitation tools, and even an operational overlap with what we originally thought was an unrelated attack campaign. The Middle East region has proven to be a hotbed of threat activity in recent times, with continued acceleration of pacing as well as development in the tactics and techniques used. There is no indication that this type of threat activity will cease, but with continued discovery of the adversary's playbooks, implementation of strong security policies, and effective deployment of technology, we can make it far less worthwhile for the adversary to execute their attacks.

Post-exploitation Tools SHA256 Hashes

28a0db561ff5a525bc2696cf98d96f443f528afe63c5097c5e0ccad071fcb8c2
744e0ce108598aaa8994f211e00769ac8a3f05324d3f07f7705277b9af7a7497
caf5f9791ab3049811e16971b4673ec6d4baf35ffaadd7486ea4c5e318d10696
6ae32cd3b5a8a1dbb5464372ded370f31802fd1f5031795b43d662c64fc5b301
3b08535b4add194f5661e1131c8e81af373ca322cf669674cf1272095e5cab95
450ebd66ba67bb46bf18d122823ff07ef4a7b11afe63b6f269aec9236a1790cd
5b7eb534a852c187eee7eb729056082eec7a028819191fc2bc3ba4d1127fbd12
6e623311768f1c419b3f755248a3b3d4bf80d26606a74ed4cfd25547a67734c7
497e6965120a7ca6644da9b8291c65901e78d302139d221fcf0a3ec6c5cf9de3
d3b03c0da854102802c21c0fa8736910ea039bbe93a140c09689fc802435ea31
5ead94f12c307438e6475e49f02bedaee0cd09ce6cebb7939f9a2830f913212c
bb9b4e088eb99100156f56bbd35a21ff7e96981ffe78ca9132781e9b3f064f44

Credential Harvesting Domains

owa-insss-org-ill-owa-authen[.]ml
webmaiil-tau-ac-il[.]ml
mail-macroadvisorypartners[.]ml
webmail-tidhar-co-il[.]ml
my-mailcoil[.]ml
logn-micrsftonine-con[.]ml
so-cc-hujii-ac-il[.]ml
