

Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford

 clearskysec.com/oilrig/

Iranian threat agent OilRig has been targeting multiple organisations in Israel and other countries in the Middle East since the end of 2015. In recent attacks they set up a fake VPN Web Portal and targeted at least five Israeli IT vendors, several financial institutes, and the Israeli Post Office.

Later, the attackers set up two fake websites pretending to be a University of Oxford conference sign-up page and a job application website. In these websites they hosted malware that was digitally signed with a valid, likely stolen code signing certificate

Based on VirusTotal uploads, malicious documents content, and known victims – other targeted organisations are located in Turkey, Qatar, Kuwait, United Arab Emirates, Saudi Arabia, and Lebanon.

Fake VPN Web Portal

In one of the recent cases, the attackers sent the following email to individuals in targeted organisations:

Subject: please help me about it::

hi,

Please login and test the rdp, then feed me back the result.
I need your feed back for making my project result as soon as possible.

[https://\[REDACTED\]dana-na/auth/url_default/welcome.cgi](https://[REDACTED]dana-na/auth/url_default/welcome.cgi)

username: [REDACTED]

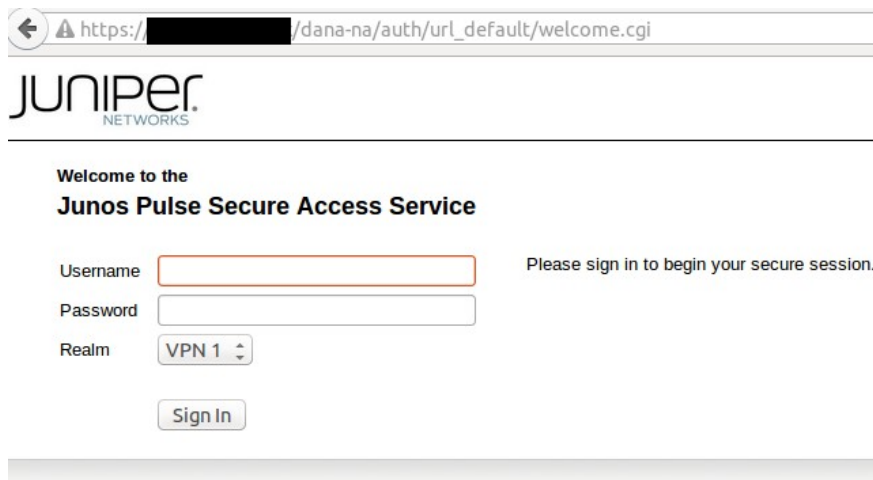
password: [REDACTED]

thanks

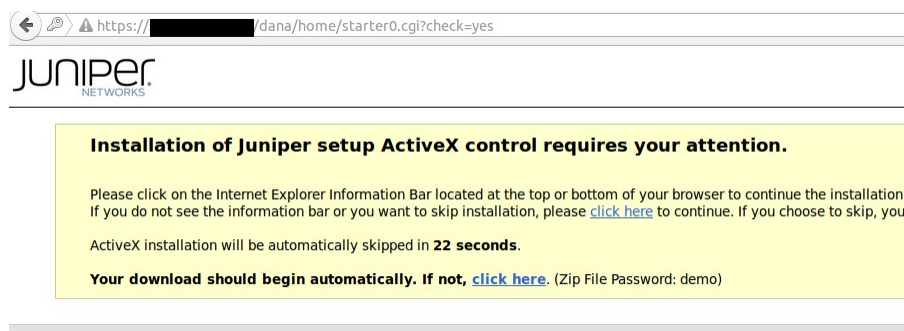
[REDACTED]

The email was sent from a compromised account of an IT vendor. Similar emails were sent from other IT vendors in the same time period, suggesting the attackers had a foothold within their networks, or at least could get access to specific computers or email accounts.

The link provided in the malicious email led to a fake VPN Web Portal:



Upon logging in with the credentials provided in the email, the victim is presented with the following page:

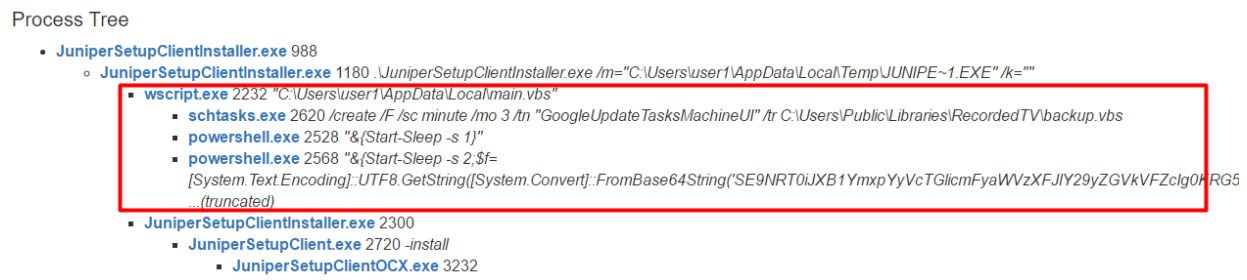


The victim is asked to install the “VPN Client” (an .exe file), or, if download fails, to download a password protected zip (with the same .exe file inside).

The “VPN Client” is a legitimate Juniper VPN software bundled with [Helminth](#), a malware in use by the OilRig threat agnet:

JuniperSetupClientInstaller.exe
6a65d762fb548d2dc56cfde4842a4d3c ([VirusTotal link](#))

If the victim downloads and installs the file, their computer would get infected, while the legitimate VPN software is installed. The legitimate and the malicious installations can be seen in the process tree when the file is run in a Cuckoo sandbox. Malicious processes are marked red (click image to enlarge):



The following malicious files are dropped and run:

- C:\ProgramData\{2ED05C38-D464-4188-BC7F-F6915DE8D764}\OFFLINE\9A189DFE\C7B7C186\main.vbs
dcac79d7dc4365c6d742a49244e81fd0

- C:\Users\Public\Libraries\RecordedTV\DnE.ps1
7fe0cb5edc11861bc4313a6b04aeedb2
- C:\Users\Public\Libraries\RecordedTV\DnS.ps1
3920c11797ed7d489ca2a40201c66dd4
- "C:\Windows\System32\schtasks.exe" /create /F /sc minute /mo 3 /tn "GoogleUpdateTasksMachineUI" /tr
C:\Users\Public\Libraries\RecordedTV\backup.vbs
7528c387f853d96420cf7e20f2ad1d32

Command and control server is located in the following domain:

tecsupport[.]in

A detailed analysis of the malware is provided in [two posts](#) by Palo Alto networks and in a [post](#) by FireEye, which wrote about previous campaigns by this threat agent.

(Note that Juniper networks was not compromised nor otherwise involved in the attack, except for the attackers using its name and publicly available software).

Digitally signed malware

The entire bundle (VPN client and malware) was digitally signed with a valid code signing certificate issued by Symantec to AI Squared, a legitimate software company that develops accessibility software:

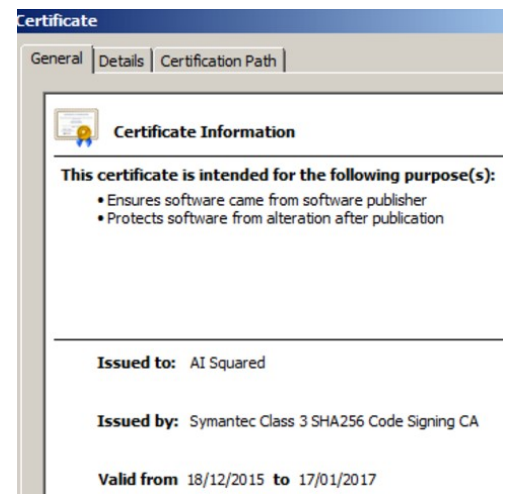
Thumbprint: F340C0D841F9D99DBC289151C13391000366631C
Serial number: 45 E4 7F 56 0B 01 B6 4E 68 39 5E 5D 79 2F 2E 09

Another Helminth sample, [1c23b3f11f933d98febfd5a92eb5c715](#), was signed with a different AI Squared code signing certificate:

Thumbprint: 92B8C0872BACDC226B9CE4D783D5CCAD61C6158A
Serial number: 62 E0 44 E7 37 24 61 2D 79 4B 93 AF 97 46 13 48

This suggest that the attackers had got a hold of an Ai Squared signing key, potentially after compromising their network. Alternatively, the attackers might have got Symantec to issue them a certificate under Ai Squared's name.

[Update 11 February 2017: In a [notification](#) in its website, Ai Squared says that "The digital certificate used to certify newer ZoomText and Window-Eyes software products has been compromised. As a result, our certificate will be revoked on or around January 26th"]



University of Oxford impersonation

The attackers registered four domains impersonating The University of Oxford.

oxford-symposia[.]com, is a fake Oxford conference registration website. Visitors are asked to download the "University Of Oxford Job Symposium Pre-Register Tool":

For Pre-Register in university of Oxford Job Symposium download Symposium Pre-Register Tool from below and send your form to us (info@oxford-symposia.com)



[Download University Of Oxford Job Symposium Pre-Register Tool](#)

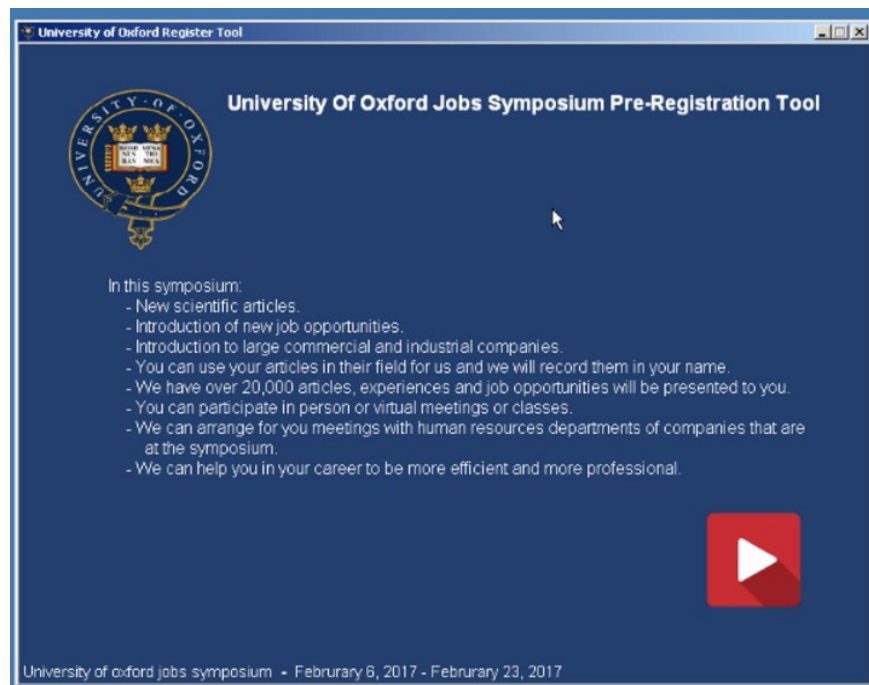


[Download University Of Oxford Job Symposium](#)

The downloaded file (which is also signed with an AI Squared certificate), is a fake registration tool built by the attackers:


OxfordSymposiumRegTool.exe
f77ee804de304f7c3ea6b87824684b33

If run by the victim, their computer would get infected, while they are shown this registration process:



University of Oxford Register Tool


Step 1: Basic informations





E-mail:

Phone Number:

Date of Birth:





University of oxford jobs symposium - February 6, 2017 - February 23, 2017

University of Oxford Register Tool

Save Your Pre-Registration Form :







Save your Pre-Registration form and send .oxr file to us.

Email: info@oxford-careers.com

We will contact you as soon as possible.

Thank you.

University of oxford jobs symposium - February 6, 2017 - February 23, 2017

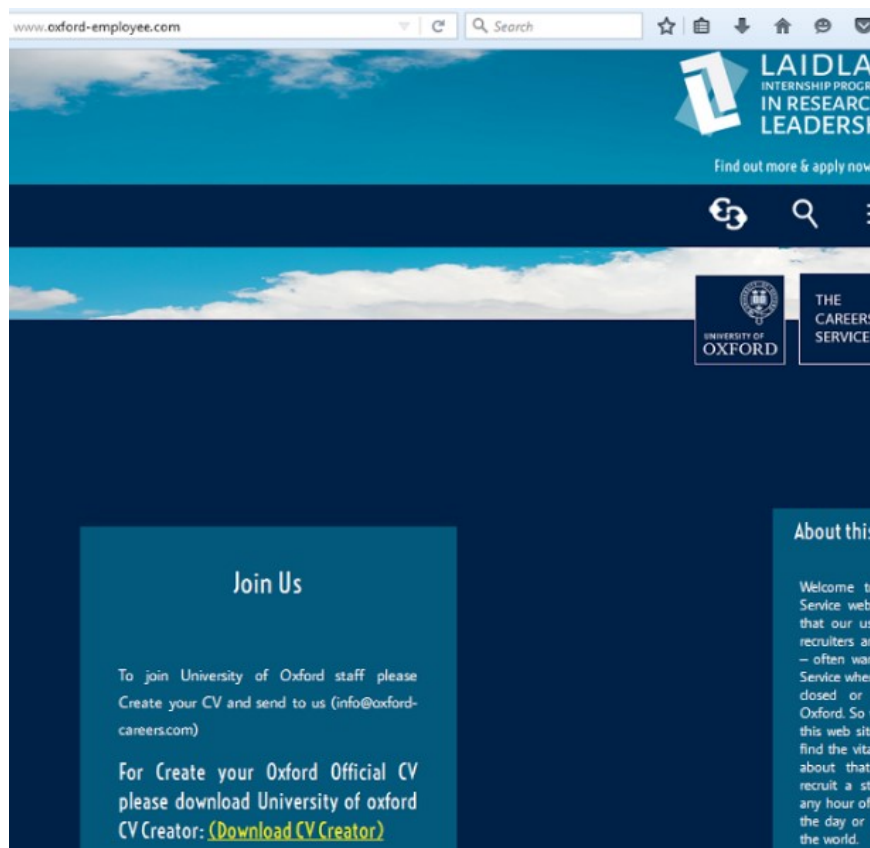
Note that after completing the “registration process”, the victim is asked to send the form to an email address in **oxford-careers[.]com**, which also belongs to the attackers.

Previously the fake website linked to the following documents in a third fake Oxford domain, **oxford[.]in**:

[http://oxford\[.\]in/downloads/ls1.doc](http://oxford[.]in/downloads/ls1.doc)
[http://oxford\[.\]in/downloads/ls2.doc](http://oxford[.]in/downloads/ls2.doc)
[http://oxford\[.\]in/downloads/ls3.doc](http://oxford[.]in/downloads/ls3.doc)
[http://oxford\[.\]in/downloads/ls4.do](http://oxford[.]in/downloads/ls4.do)

The documents were unavailable during our research, and their content is unknown to us.

The attackers used a forth domain, **oxford-employee[.]com**, to host an “Oxford Job application” website:



Visitors are asked to “Download CV Creator” in order “To Join University of Oxford staff”. CV Creator is a malicious file hosted at [http://www.oxford-careers\[.\]com/Files/OxfordCVCreator.exe](http://www.oxford-careers[.]com/Files/OxfordCVCreator.exe) :

OxfordCVCreator.exe

5713c3c01067c91771ac70e193ef5419

When run, the victim is again presented with a tool created by the attackers, this time a “University Of Oxford Official CV Creator”:



Both samples mentioned in this section had the following domain used for command and control:

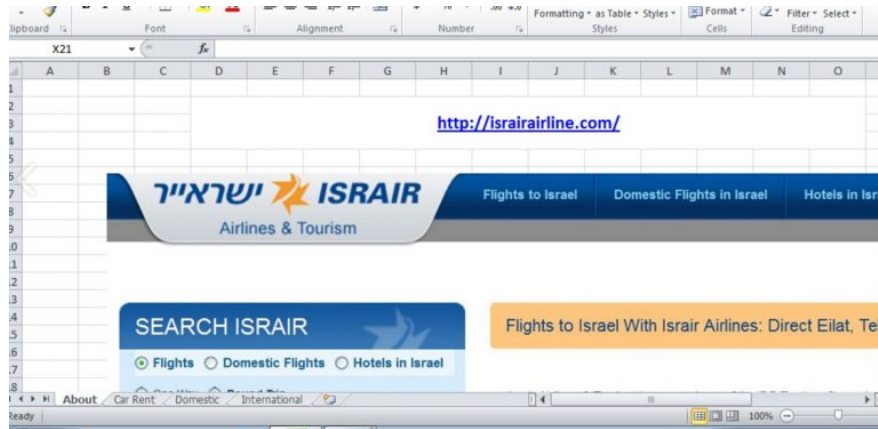
updater[.]li

Other incidents

In an earlier incident, the attackers sent a malicious excel file impersonating Isirair, an Israeli Airline (the content of the file was copied from the company's public website and we have no indication of it being compromised or targeted):

Israel Airline.xls

197c018922237828683783654d3c632a



The file had a macro that if enabled by the user would infect its computer.

In other incidents the attackers used the following files:

- Special Offers.xls / Salary Employee 2016.xls
f76443385fef159e6b73ad6bf7f086d6
- pic.xls
3a5fcba80c1fd685c4b5085d9d474118

A screenshot of a Microsoft Excel spreadsheet displaying a promotional offer for Dubai Flydubai. The spreadsheet has a header row with columns C through L. Below the header, there is a grey bar with the text 'more info at www.flydubai.com/en/offers'. The main content area is divided into two columns, each featuring a night-time photograph of the Dubai skyline. Below each photograph is a light blue box containing the text 'Dubai DXB' and 'Dubai DWC' respectively. At the bottom, there are two tables, each with a green border. The first table is for 'Dubai DXB' and the second is for 'Dubai DWC'. Both tables have a header row labeled 'Economy Class' and two data rows: 'Was USD 220' and 'Now USD 170' for DXB, and 'Was USD 220' and 'Now USD 167' for DWC.

Economy Class	
Was USD 220	Now USD 170

Economy Class	
Was USD 220	Now USD 167

- People List.xls
bd7d2efdb2a0f352c4b74f2b82e3c7bc
- cv.xls
72e046753f0496140b4aa389aee2e300
- users.xls
262bc259682cb48ce66a80dcc9a5d587
- Employee Engagement Survey.xls
726175e9aba421aa0f96cfc005664302
- JuniperSetupClientInstaller.exe
f8ce7e356e09de6a48dca9e51421b6f6
- Project_Domain_No337.chm
1792cdd0c5397ff5df445d73276d1a50 ([undetected as malicious by any antivirus on VirusTotal](#))
- gcaa_report_series15561.chm
d50ab63f4034c6f5eb356e3326320e66 ([undetected as malicious by any antivirus on VirusTotal](#))

Infrastructure overlap with Cadelle and Chafer

In December 2015, Symantec published a [post](#) about “two Iran-based attack groups that appear to be connected, Cadelle and Chafer” that “have been using Backdoor.Cadelspy and Backdoor.Remexi to spy on Iranian individuals and Middle Eastern organizations”.

Backdoor.Remexi, one of the malware in use by Chafer, had the following command and control host:

87pqxz159.dockerjsbin[.]com

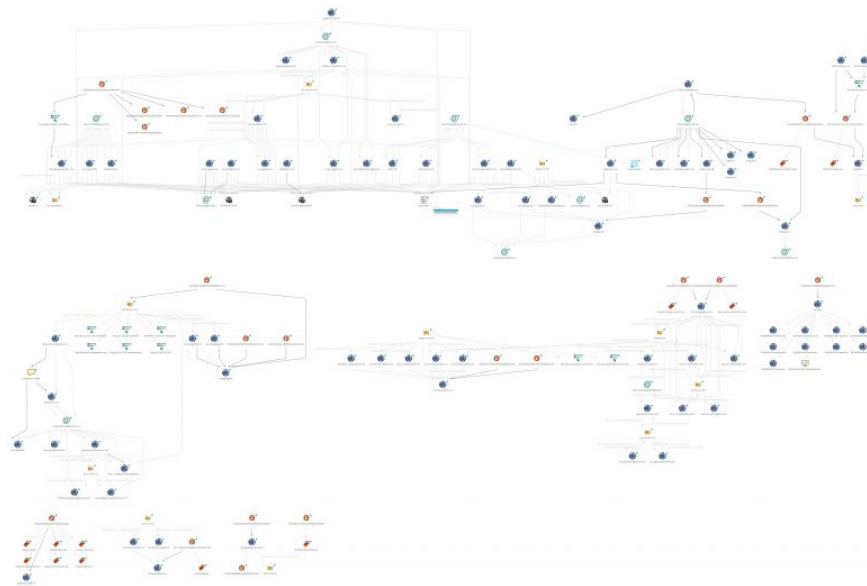
Interestingly, IP address 83.142.230.138, which serve as a command and control address for an OilRig related sample (3a5fcba80c1fd685c4b5085d9d474118), was pointed to by 87pqxz159.dockerjsbin[.]com as well.

This suggest that the two groups may actually be the same entity, or that they share resources in one way or another.

Indicators of compromise

Indicators file: [oilrig-indicators.csv](#) (also available on [PassiveTotal](#))

The graph below depicts the OilRig infrastructure (click to enlarge):



Acknowledgments

This research was facilitated by [PassiveTotal](#) for threat infrastructure analysis, and by [MalNet](#) for malware research . We would like to thank [White-Hat](#), Tom Lancaster of [Palo Alto Networks](#), Michael Yip of [Stroz Friedberg](#), security researcher Marcus, and other security researchers and organizations who shared information and provided feedback.