Cybersecurity for Everyone Course Final Project: OilRig

Hackers are not all the same; they range in skill, resources, and capability and often go by different names. How would you classify this threat actor? Do they go by any aliases? Where are they from? How would you rate the skill level and resources available to this threat actor?

- OilRig is an Iranian government backed group that is classified as an Advanced Persistent Threat (APT) mainly because of their numerous attacks with varying degrees of success. They are also known by different names such Cobalt Gypsy, IRN2, Helix Kitten, Twisted Kitten and APT34.

- In a Forbes report, the Counter Threat Unit of the cyber intelligence firm SecureWorks is certain that OilRig is working for the Iranian government while the Israeli IT firm ClearSky traced the group back to Iran. Most of their operations are within Middle East but they also had success outside the region and while most Iranian threat actors target government agencies and dissidents, OilRig focuses on private industries outside of Iran.

- Since OilRig is working with/for (Islamic Republic of) Iran, they are sure to have enough resource to conduct any operation that is expected to be beneficial for Iran. Like the Mabna Institute case, where an Iranian organization (Mabna Institute) was subcontracted by the Islamic Revolutionary Guard Corps to conduct a massive spear phishing campaign that resulted to a total stolen value of $3.4 billion worth of Intellectual Property (IP) and 31.5 terabytes of academic data.

Hackers are motivated to act for specific reasons. What are the motivations of your threat actor? What is the specific geo-political context they are operating in and what insight does that give you for why they are operating in this manner?

According to Council on Foreign Relations, OilRig targets private-sector and government entities for the purpose of espionage. Merriam-Webster defines Espionage as the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company. The Cambridge Business English Dictionary define it as the activity of secretly collecting and reporting information, especially secret political, military, business, or industrial information.

In a geo-political context, Iran has always disagreed with their neighbors in the region and Western countries because of many reasons and according to the Middle East Institute (MEI) "because of the Iranian Revolution of 1979, many countries stopped business with Iran and so stealing academic and corporate information from around the globe allows it to renew infrastructure and build technologies that it simply cannot purchase abroad, ranging from weaponry to airplane parts."

Iran's effort to tell their side of the story on issues is also not that popular and because Iran is suffering from economic sanctions imposed on them, they rely on what described by many as "soft war" (less regulated and low-level conflict for extended periods of time) in the cyber space with public and private sectors in rival countries as their target.

MEI also assessed that Iran-linked actors are likely to focus on two cyber operations in the medium and long term:
foreign election meddling and widespread theft of intellectual property (IP).

Sample Cases of OilRig attacks: The Hacking Process tactics on their targets and the Primary, Secondary and Second Order Effects

Case 1 - OilRig attack using AI Squared software

Case 2 - OilRig attack impersonating Oxford University

Case 3 - OilRig attack on Al Elm and Samba Financial Group

Case 4 - OilRig attack on Job Hunters

Case 5 - OilRig attack on Israeli IT vendors

Case 1 - OilRig attack using AI Squared software

A small, mission-driven tech firm AI Squared based in Vermont developed a software that alters websites to help the visually impaired use the internet.

Forbes reported that, AI Squared received a warning from security giant Symantec that certificates for technology that are designed to guarantee its authenticity had been compromised, suggesting that a threat actor (OilRig) got hold of AI Squared's signing key and certificates which they used to disguise their own malware.

The goal was to make use of the software for the visually impaired as their surveillance tool and make it appear legitimate to security systems of their many targets across the Middle East, Europe and the U.S.

As a result, on an AI Squared website notification in 2017 says that their certificate has been revoked because the digital certificate used to certify newer ZoomText, and Window-Eyes software products has been compromised.

Case 1 - OilRig attack using AI Squared software

Reconnaissance - The group has a wide range of target on the Middle East, Europe, and the US and OilRig thought that AI Squared tech firm has the software to help them reach their victims with ease.

Weaponization - OilRig is assumed to already have control over AI Squared's signing key and certificate and used the legitimate software as their own malware.

Delivery - Because of human compassion on assisting visually impaired to access the internet, most have considered to use the (already compromised) software by AI Squared.

Exploitation and Installation - People are bound to install and use the software on their computers to see if it is effective.

Command & Control - The victims who use the software (malware) are unknowingly feeding information to the OilRig group which can then help them gain access to bigger networks.

Primary Effect - Exploitation of End Host

- OilRig has infected a software for the visually impaired with their malware for surveillance purposes

Secondary Effects on Revenue, Reputation and Macroeconomics

- Revenue - Since the software is infected with OilRig's surveillance malware purchase would now be lower than expected
- Reputation - Customers would then find a different software that offers the same kind of service
- Macroeconomics - Because of the software getting infected,
  there could be change of personnel who work on the software

Second Order Effect on Information / Perception

- Everybody who already has access to the software might think that the company is a front for spying purposes

Case 2 - OilRig attack impersonating Oxford University

ClearSky reports that the OilRig group has created and registered two (2) fake Oxford University pages in November 2016, one claims to offer a job inside the institution, and the other is a conference sign-up website.

Both pages encouraged the visitors to download files. One file is a requirement to complete a registration for the fake event and the other file is an Oxford University CV creator. Once clicked, victims are unknowingly feeding information to the OilRig's malware, named Helminth, allowing them to control the PC and steal data.

Case 2 - OilRig attack impersonating Oxford University

Reconnaissance - OilRig is interested in hitting many targets at one operation and so they created fake Oxford University websites for their plan

Weaponization - OilRig created 2 fake Oxford University websites; one claiming to offer jobs and the other is a registration site for a conference.

Delivery - People who are interested in working for or attending a conference hosted by Oxford are sure to follow the bogus page requirements

Exploitation and Installation - The victims, once on the fake website/s are encouraged to fill-up what seem to be a normal registration form and download files that are infected by OilRig's surveillance malware.

Command & Control - Because people have registered and downloaded files from the fake websites, OilRig now have collected their victim's basic information and gained access to the computers infected with Helminth malware.

Primary Effect - Exploitation of End Host

- OilRig thought of collecting personal information through the fake Oxford Website they created.

Secondary Effect on Reputation

- Reputation - Oxford University's reputation is sure to be affected because their name and identifiers are used in the fake website

Second Order Effect on Information / Perception

- It is an unfortunate event but everybody who sent personal information and registered in the fake Oxford websites would now pick different universities to be associated with.

Case 3 - OilRig attack on Al Elm and Samba Financial Group

According to a Forbes report on 2017, phishing attempts were launched by the group on May 2016 from servers within Saudi Arabian contractor and IT security Al-Elm.

The email was injected into a thread between Al-Elm and one of Saudi Arabia's lender, Samba Financial Group. The email contained a version of OilRig's Helminth surveillance kit, which would launch as soon as a recipient opened an attached document, in this case an Excel file called "notes.xls."

In the case of Al-Elm, analysis of the headers of the phishing emails indicated they originated from within the sender's organization and "the threat actor previously compromised those organizations," according to SecureWorks intelligence analyst Allison Wikoff

Case 3 - OilRig attack on Al Elm and Samba Financial Group

Reconnaissance - The target here is the Samba Financial Group which has reported $290 million profit from last quarter of the previous year

Weaponization - The OilRig group chose to use the "previously compromised" network of Al-Elm to establish a connection with Samba Financial Group

Delivery - An email with the OilRig's Helminth surveillance kit was injected into a thread of email between Al-Elm and Samba Financial Group

Exploitation and Installation - Once the email has been sent, people who open the attached excel file named "notes.xls" will have their computer infected with the Helminth surveillance kit.

Command & Control - Everything might seem normal after opening the email but once the surveillance kit has been installed, OilRig has now gained access to that computer and possibly the company's network.

Primary Effect - Exploitation of End Host

- Through phishing attempts, OilRig has sent an email with Helminth surveillance kit to Al-Elm Security and Samba Financial Group

Secondary Effects on Remediation / Reputation

- Remediation - The infected devices from both ends would now be scanned, cleaned and possibly replaced depending on how much it got affected
- Reputation - The reputation of the IT security firm is to be affected because they are supposed prevent threat actors from getting in between them and their clients

Second Order Effect on Information / Perception

- Because of the phishing emails sent, both companies would now be very cautious in doing future business partnership.

Case 4 - OilRig attack on Job Hunters

From the same report from previous case, cyber intelligence firm SecureWorks who calls the OilRig crew Cobalt Gypsy said that the group has been sending out messages loaded with malware from legitimate email addresses belonging to one of Saudi Arabia's biggest IT suppliers, the National Technology Group, and an Egyptian IT services firm, ITWorx.

From those email accounts, an unnamed Middle East entity was targeted with messages promising links to job offers. Hidden in the attachments was PupyRAT, an open-source remote access trojan (RAT) that works across Android, Linux and Windows platforms.

Case 4 - OilRig attack on Job Hunters

Reconnaissance - The OilRig's target is an unnamed entity but they chose to launch the attack on the Middle East

Weaponization - OilRig group chose to use Saudi Arabia's IT supplier, National Technology Group and Egypt's IT service firm ITWorx to send an email loaded with malware.

Delivery - OilRig used email addresses belonging to the IT firms to send enticing job offer to their victims.

Exploitation and Installation – When receivers open the email, hidden in the email link attachments was an open-source remote access trojan.

Command & Control - Once the link has been accessed, the malware would then begin the process of collecting credentials from the user and the computer.

Primary Effect - Exploitation of End Host

- OilRig has sent emails from legitimate IT firms to various targets with links to job offers which is infected with an open-source remote access trojan

Secondary Effect on Reputation

- Reputation - The job offers might be legitimate, but the job hunters would now think twice on joining the IT firms because they would trace the source of the PupyRAT to their devices from links inside the email.

Second Order Effect on Information / Perception

- The firms might get the reputation of spying on their current and future employees and customers.

Case 5 - OilRig attack on Israeli IT vendors

- According to the ClearSky research team, OilRig has sent emails to several targeted Israeli IT Vendors using a compromised account. It is a basic email requesting help with details of the supposed customer and when logging in with the credentials the victim is asked to install a legitimate Juniper VPN software bundled with Helminth; a malware commonly used by the group for surveillance purposes.

Case 5 - OilRig attack on Israeli IT vendors

- Reconnaissance - The OilRig's target is Israel and they think that attacking IT vendors could help them infiltrate important networks
- Weaponization - It is assumed that OilRig already has access to compromised customer accounts from various Israeli IT vendors.
- Delivery - The group sends an email to the vendors disguising themselves as legitimate customers asking for help.
- Exploitation and Installation - When the victims try to access the user's account with their provided credentials, the victim is then asked to download a Juniper VPN to proceed. The legitimate Juniper VPN they provide is bundled with their surveillance malware Helminth.
- Command & Control - When successfully installed, OilRig would then have access to the device and many other client/customer emails that use their services.

- Primary Effect - Exploitation of End Host
  - OilRig would be interested in infiltrating Israeli networks, and so they disguised themselves as customers who need assistance
- Secondary Effect on Remediation
  - Remediation - Because it is their job to keep customers satisfied, some employees of the firms might have followed the threat actor's instructions. As a result, firms may have to check, clean and/or replace their devices
- Second Order Effect on Information / Perception
  - Because the malware Helminth is attached to a legitimate Juniper VPN, people who use the VPN might be worried that their devices are infected with the surveillance malware too.

Not all hackers represent a strategic problem for policy makers. How would you characterize your threat actor, are they chiefly a private problem for businesses or a public concern for policy makers? How should policy makers respond?

OilRig is clearly an Advanced Persistent Threat (APT) because of the range of their targets. Their main activity is espionage, they do not engage in destroying, wiping, or altering whatever they get an access to, but instead they just sit back and relax while their Helminth malware does its job. Most of their espionage activities have resulted in stolen information using compromised email.

OilRig is interested in targeting private industries and their tactics are very subtle, mostly through phishing. They are a clear threat to businesses but because these companies have connections with private citizens, public and other types of institutions, one email could be their way into a government office or a corporate giant, making them both a private problem and a public concern for policy makers. Since OilRig has been identified as a threat actor from Iran, imposing more economic sanctions would be the appropriate response. One country could only do so much to try and get Iran to pay for any harm done through cyber espionage. It is possible but might be a really long process and when any secrets are compromised, it could never be replaced.

Policy makers could also make a collective effort to punish and discourage threat actors through treaties, it could be with Iran if they accept or with countries that also have an issue with threat actors from Iran. If a group of countries want to make a different version of the Iran Nuclear Deal in the future, it should not include any monetary incentives but instead, there should be clear punishments for any cyber related activities like espionage coming from any group that could be traced back or is sponsored by Iran.

Resources

https://attack.mitre.org/groups/G0049/

https://www.forbes.com/sites/thomasbrewster/2017/02/15/oilrig-iran-hackers-cyberespionage-us-turkey-saudi-arabia/?sh=4c88925f468a

https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

https://microsites-live-backend.cfr.org/interactive/cyber-operations/oilrig
https://www.merriam-webster.com/dictionary/espionage

https://dictionary.cambridge.org/us/dictionary/english/espionage

https://www.mei.edu/publications/irans-cyber-future

https://www.clearskysec.com/oilrig/

https://www.cfr.org/backgrounder/what-iran-nuclear-deal