WAPACK LABS
CYBER INTELLIGENCE SERVICE

TLP GREEN

TACTICAL CYBER INTELLIGENCE REPORT

Serial: TR-19-037-001
Report Date: 02062019

Oil and Gas Sector Phishing

Summary

Three (3) oil and gas (Energy) sector companies were the target of attempted phishing campaigns from a Malawi, Africa identified malicious domain.

Virus Total identified malicious domain:[1]

etcay.org domain information:
Description: Economic and Trade Cooperation of African Youth (ETCAY), Monrovia, Liberia; P.O Box 100 +231-777-270-104 · info@etcay.org ETCAY was formed by the delegates at the 3rd China-Africa Youth Festival representing 53 African countries. Etcay.org site is currently down. Passive DNS replication (This domain has been seen to resolve to the following IP addresses.)

2019-02-04	50.116.98.247
2019-01-16	162.241.232.23
Domain Name:	ETCAY.ORG
Reg. Domain ID:	D402200000007927624-LROR
WHOIS Server:	http://api[.]fastdomain.com/cgi/whois
Registrar URL:	http://www[.]fastdomain.com
Updated Date:	2018-12-11T03:45:19Z
Creation Date:	2018-10-11T09:36:25Z
Reg. Expiry Date:	2019-10-11T09:36:25Z
Registrar:	FastDomain Inc.
Registrant Country:	MW (Malawi)
Name Server:	NS1&2[.]NZATHU.NET
Reg. IANA ID: 1	154

These phishing attempts were detected in Wapack Labs Threat Recon malicious domain (URL) collections, and were used in phishing campaigns against Enbridge Inc. (Canada), Range Resources (US) and Targa Resources (US); all oil and gas sector companies. The malicious domain "etcay.org" appears to have been originally a legitimate domain, then taken over by a malicious actor(s) in Malawi, Africa. There was no specific malware detected with these phishing attempts and appear to be social engineering attempts. These phishing campaigns demonstrate active targeting of energy sector companies by identified and known malicious sites.

[1] Virus Total's passive DNS only stores address records. The domain etcay.org has been seen to resolve to the following IP addresses: 50.116.98.247, and 162.241.232.23

Targets and Threat

On 5 February 2019, Wapack Labs identified phishing attacks through Virus Total collection, targeting oil and gas industry companies.

Enbridge Incorporated

http://www[.]enbridge.com
Description: Enbridge Inc. is a Canadian multinational energy transportation company based in Calgary, Alberta. It focuses on the transportation, distribution and generation of energy, primarily in North America.

Stock price (02/06/2019):	ENB (NYSE) $37.68 +0.03 (+0.08%)
Headquarters:	Calgary, Canada
CEO:	Al Monaco
Revenue:	32.9 billion CAD
Subsidiaries:	Union Gas, MORE

Figure 1. Cxxxxa LinkedIn

Phishing emails were sent from encay.org to armando.corona@enbridge.com. Mr. Cxxxxa is a real person and is a Senior Auditor for Enbridge Inc. A second email was sent to: Jenna.Johnson@enbridge.com. The last name of Johnson may be spoofed of a similar position and name, who is an employee of Enbridge. The third email targeted: denise.janxxxxk@ enbridge.com. Ms. Janousek is an investment evaluator for Enbridge Inc.

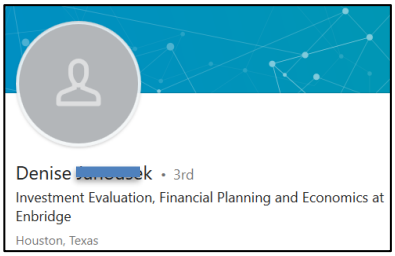

Figure 2. Janxxxxk LinkedIn

Range Resources

http://www[.]rangeresources.com/
Range Resources Corporation is a petroleum and natural gas exploration and production company organized in Delaware and headquartered in Fort Worth, Texas. It is one of the largest exploration companies operating in the US.
Stock price (2-5-2019): RRC (NYSE) $10.26 -0.46 (-4.29%)
Headquarters: Fort Worth, TX
CEO: Jeffrey L Ventura
Revenue: 2.611 billion USD (2017)
Subsidiaries: RANGE RESOURCES APPALACHIA LLC

Phishing emails were sent from encay.org to bmiller@rangeresources.com. There is an A. Miller, Geologist at Ranger Resources; but no B. Miller. This may be a spoof attempt to phish a victim.

Targa Resources

http://www[.]targaresources.com
Targa Resources is a Fortune 500 company based at 811 Louisiana, formerly known as Two Shell Plaza, in Houston, Texas. Targa is a midstream energy corporation and one of the largest providers of natural gas and natural gas liquids in the US.
Stock price (2-5-2019): TRGP (NYSE) $43.92 -0.01 (-0.02%)

Headquarters: Houston, TX
CEO: Joe Bob Perkins
Number of employees: 2,130 (2017)
Subsidiaries: Targa Resources LLC

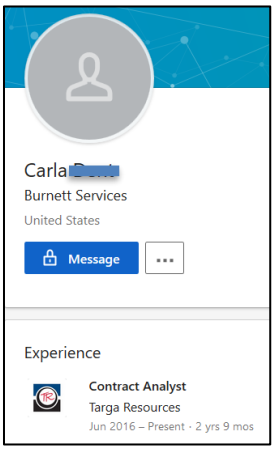

Figure 3. Xxxx LinkedIn

Phishing email was sent from encay.org to cXxxx@targaresources. There is a Carla XXX, Contract Analyst with Targa Resources.

Virus Total analysis identified this phishing as malicious credential content, attempting to steal Microsoft account password identifiers. The same malicious domain (etcay.org) targeted several other high-profile emails belonging to a US bank and a large US insurance provider.

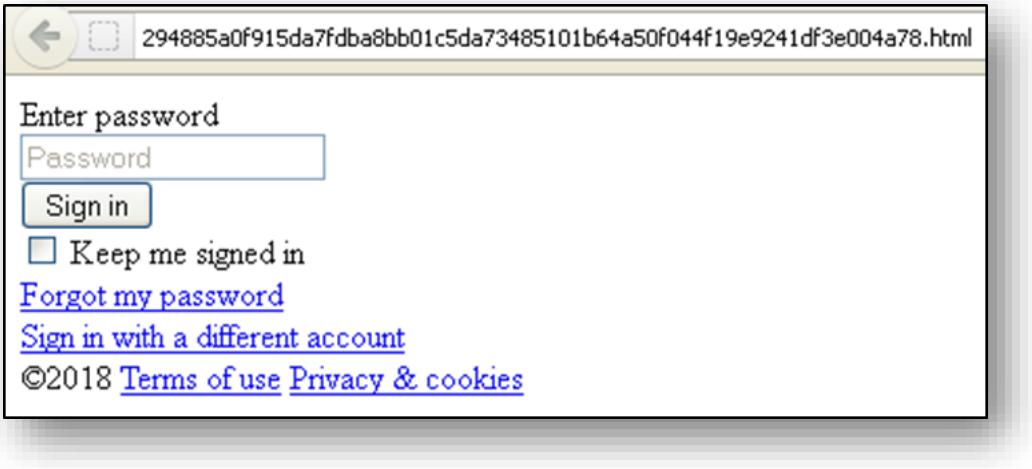

Figure 4. Microsoft account login and password

The likely objective for the bad actors was to steal the Microsoft account password. An additional campaign that was hosted on etcay.org began on 9 January 2019. Under the pretense of an invoice in the cloud, actors were asking for login credentials giving the target a variety of "login" options (Figures 4, 5).

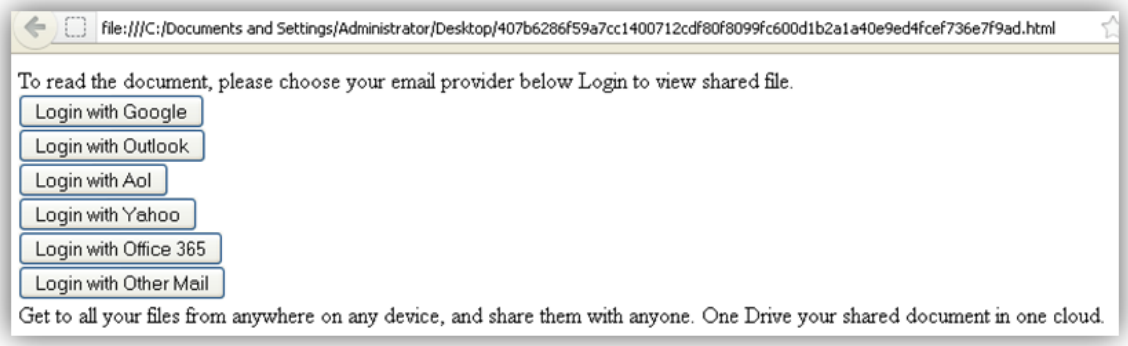

Figure 5. Separate phishing content download from etcay.org

Actors using phishing pages identical to the one that targeted these oil and gas sector companies regularly move to new domains. As of 6 February 2019, two new domains are reported:

2019-02-06 http://collecaicvice.uk/portal/microsoft/
2019-02-06 http://iamservices.com/portal/microsoft/

Conclusion:

Our collection and analysis indicate the willingness of bad actors to corrupt domains in order to social engineer the oil and gas sector to obtain login and password credentials. Oil and gas sector companies should train and caution employees to be aware of this continuous threat. If these phishes are successful, the loss of vital proprietary information could be detrimental to the company.

For questions or comments regarding this report, please contact the Lab directly by at 844-4-WAPACK (1-844-492-7225), or feedback@wapacklabs.com