New Insights into Energetic Bear's Watering Hole Cyber Attacks on Turkish Critical Infrastructure

riskiq.com/blog/labs/energetic-bear/

November 2, 2017

Labs

November 02, 2017

By Yonathan Klijnsma

On October 20th US-CERT published an alert (TA-17-293A) with information about the activities of an APT targeting the critical infrastructure sector. The report contains an extensive set of indicators with detailed context and information around them. Part of the Russian sphere of influence, the threat group discussed in the US-CERT report is the perpetrator of documented cyber espionage attacks around the world, many of which target industrial and manufacturing firms and critical infrastructure. Known by many names, the group is most prominently known as 'Energetic Bear' and 'Crouching Yeti.'

Detailed analysis of Energetic Bear's malware and activities was recently done by Kaspersky, and RiskIQ initially investigated them earlier this year. Through our web crawling network, we were able to determine that a website belonging to a Turkish energy company was being used in a watering hole attack targeting people associated with Turkish critical infrastructure. Compromised via a supply chain attack, the site was injected with SMB

credential-harvesting malware. RiskIQ then linked the malicious infrastructure to a string of related Turkish sites that were compromised for the same purpose and traced the attack back to a likely timeframe in which it began.

Watering hole attacks, especially those involving supply chain compromises, have been an extremely effective method for operators of cyber espionage campaigns because they target victims of specific groups, organizations, and regions, and with close but tumultuous relations between Turkey and the Russian Federation, Turkey is not a surprising target for Energetic Bear. We shared our findings with law enforcement and national CERT partners, but now that the indicators have become public per US-CERT's publication, we want to give our unique point of view on the threat.

Strategical Compromise for Reconnaissance

Part of Energetic Bear's campaign involved strategical web compromises that give them exposure to specific targets. For example, prior activities from the group include compromising software suppliers for programmable logic controller (PLC) components used in critical infrastructure and backdooring them with the Havex malware. In the case of the campaign described in the US-CERT report, the group compromised the website of Turcas Petrol, a Turkish energy company, located at turcas.com.tr.

Fig-1 turcas.com.tr

In May 2017, during one of our crawls of Turcas' website, RiskIQ encountered a watering hole setup in use by Energetic Bear. In the screenshot of the website above, you can see four top elements: 'Join the Turcas Energy Family,' 'Announcements,' 'Company News,' and 'Tv interviews.' These separate elements are structured as iframes to other pages on the website as shown in the DOM capture below:

Fig-2 DOM capture showing the modified subsection

However, the iframe'd page for the 'Announcements' subsection was modified by Energetic Bear operators to contain a small addition in the form of an image inclusion:

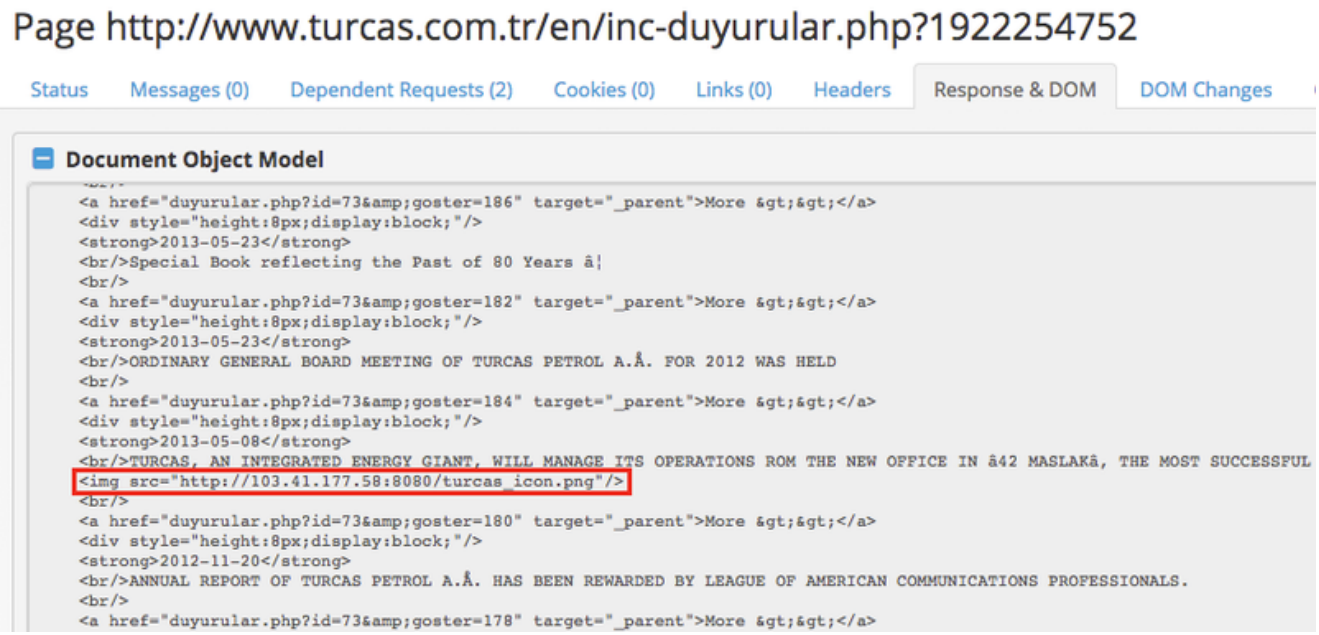
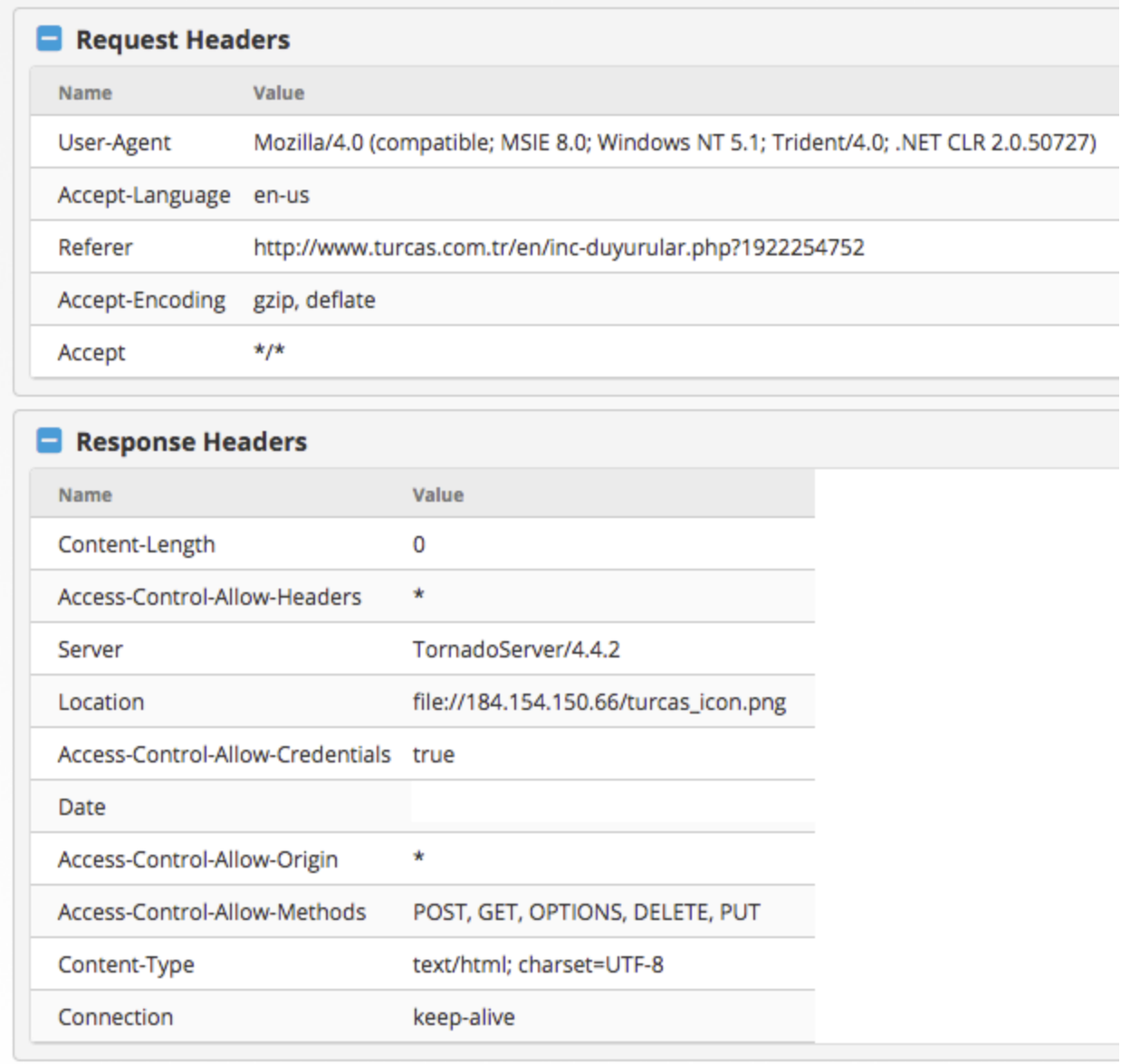


Fig-3 Malicious image inclusion

The image URL redirects to a link using the file:// scheme, which forces the connection through the file protocol, which then allows the group to harvest Microsoft SMB credentials. This behavior was also noted by Talos, which wrote a detailed analysis of the spear-phishing

emails belonging to the same campaign as this watering hole attack. It's interesting to note that the back-end server used in the attack seems to be written using the TornadoServer Python framework used for building web and networking applications:



Request Headers

Name	Value
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727)
Accept-Language	en-us
Referer	http://www.turcas.com.tr/en/inc-duyurular.php?1922254752
Accept-Encoding	gzip, deflate
Accept	*/*

Response Headers

Name	Value
Content-Length	0
Access-Control-Allow-Headers	*
Server	TornadoServer/4.4.2
Location	file://184.154.150.66/turcas_icon.png
Access-Control-Allow-Credentials	true
Date	
Access-Control-Allow-Origin	*
Access-Control-Allow-Methods	POST, GET, OPTIONS, DELETE, PUT
Content-Type	text/html; charset=UTF-8
Connection	keep-alive

Fig-4 Response headers showing the back-end server

In the case of Turcas Petrol, below is the entire chain of events we observed during the crawl:

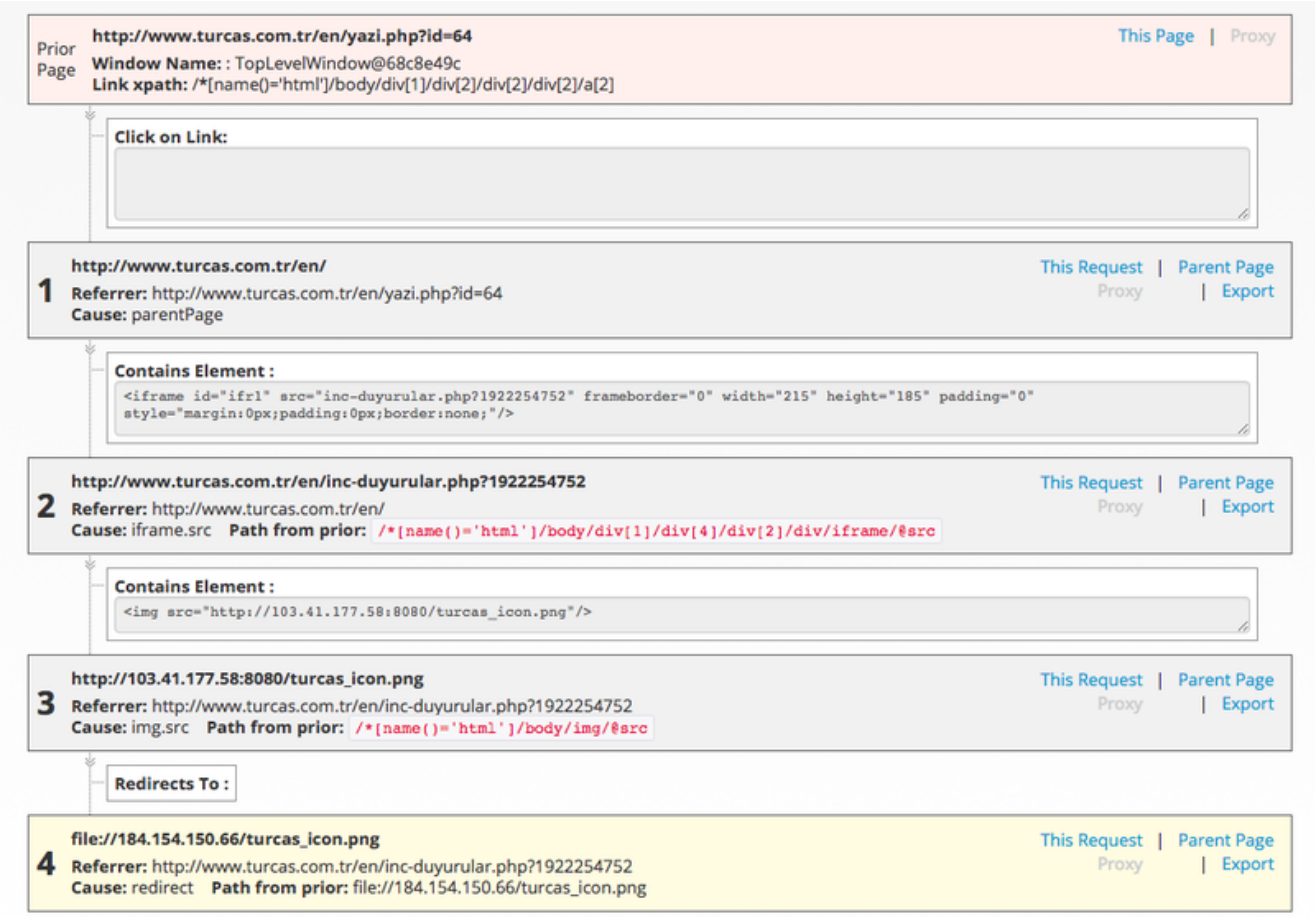


Fig-5 The entire chain of events observed by RiskIQ

In and of itself, this compromise seems targeted at Turcas Petrol and those with a close relationship with the business, a tactic that mirrors other Energetic Bear campaigns. Essentially, the group's goal is to influence areas of interest to the Russian Federation. What we'd like to show, which seems to be missing from the US-CERT report, is the entire chain of events for this attack.

RiskIQ found that the SMB credential harvesting host at 184.154.150.66 is not always directly included on the websites. Instead, the intermediary host at 103.41.177.58 is usually present on the web pages, which, in turn, redirect visitors—most likely with some filtering to avoid unwanted traffic—to the SMB harvesting host. Additionally, the URL format of the file requested, which in this case was turcas_icon.png, is not related to the referring website. Instead, Energetic Bear seems to use a form of tagging to correlate any possible victims and their source website. The format we observed is <tag>_icon.png and <tag>.png.

Strategical Compromise for Broad Targeting

The previous example of the Turcas Petrol website compromise showed specific targeting. While company-specific websites were compromised in this campaign, 'general purpose' websites were also amongst the victims. One such site is plantengineering.com which serves as an information and news hub for the critical infrastructure sector.

Fig-6 Another compromised website linked to the attack

For a few months in early 2017, this website had one of its resources compromised, likely meaning that Energetic Bear operators had broad access to the server. On the main page of the website, a resource loads from /typo3conf/ext/t3s_jslidernews/res/js/jquery.easing.js as seen in our crawl:

Fig-7 Compromised resource

The compromised resource is a modified version of jQuery Easing JavaScript library. At the bottom of the script, we can find the SMB credential harvesting link, which is embedded as an image element in the main page's DOM:

Fig-8 SMB credential harvesting link

When we go through more of our data for this very simplified direct image inclusion, we find a pattern in the URLs and websites. Here are three of our hits:

https://www.plantengineering.com/typo3conf/ext/t3s_jslidernews/res/js/jquery.easing.js
https://www.csemag.com/typo3conf/ext/t3s_jslidernews/res/js/jquery.easing.js
https://www.controleng.com/typo3conf/ext/t3s_jslidernews/res/js/jquery.easing.js

All three URLs are the same, as is the injected content. All the affected websites are news and information websites for the industrial sector, which indicates a definite pattern. So, who owns these websites? Looking at the WHOIS information in PassiveTotal we find plantengineering.com is owned by CFE Media LLC:

RECORD FROM 2017-09-13

Checked by RiskIQ | Expires in 4 years | Created 20 years ago

Attribute	Value
WHOIS Server	whois.networksolutions.com
Registrar	NETWORK SOLUTIONS, LLC.
Email	srourke@cfemedia.com (registrant, admin, tech)
Name	CFE Media LLC (registrant, admin, tech)
Organization	CFE Media LLC (registrant, admin, tech)
Street	1111 W 22ND ST STE 250 (registrant, admin, tech)
City	OAK BROOK (registrant, admin, tech)
State	IL (registrant, admin, tech)
Postal	60523-7405 (registrant, admin, tech)
Country	UNITED STATES (registrant, admin, tech)
Phone	16302770265 (registrant, admin, tech)
NameServers	ns1.grand-central.net ns2.grand-central.net ns3.grand-central.net

Fig-9 WHOIS record for affected sites

Reading a bit further, we find the email address srourke@cfemedia.com was used to register the domain. Pivoting off this address we can see the same pattern that we saw with the URLs:

Focus	Email	Registered	Expires
cfetechnology.com	srourke@cfemedia.com	2015-12-22	2017-12-22
oilandgasengrg.com	srourke@cfemedia.com	2014-09-15	2017-09-15
oandgengineering.com	srourke@cfemedia.com	2014-09-15	2019-09-15
oilngasengineering.com	srourke@cfemedia.com	2014-09-15	2019-09-15
oilandgaseng.com	srourke@cfemedia.com	2014-09-15	2017-09-15
marketingtoengineersblog.com	srourke@cfemedia.com	2014-06-23	2018-06-23
modernmarketerblog.com	srourke@cfemedia.com	2014-02-11	2018-02-11
globalplantengineering.biz	slrourke@gmail.com	2013-09-12	2014-09-11
cfemedia.com	srourke@cfemedia.com	2010-03-20	2018-03-20
globalplantengineering.com	srourke@cfemedia.com	2008-08-26	2018-08-26
sustainablemanufacturing.net	slrourke@gmail.com	2008-08-24	2015-08-24
sustainable-mfg.com	slrourke@gmail.com	2008-08-24	2015-08-24
sustainableeng.com	slrourke@gmail.com	2008-08-24	2015-08-24
purepowermagazine.com	srourke@cfemedia.com	2004-05-16	2022-05-16
controleng.net	srourke@cfemedia.com	1999-08-08	2018-08-08
plantengineering.com	srourke@cfemedia.com	1998-04-21	2022-04-20
csemag.com	srourke@cfemedia.com	1995-10-05	2017-10-04
controleng.com	srourke@cfemedia.com	1995-09-15	2017-09-14

Fig-10 Other affected sites

From our data, RiskIQ found that controleng.com, plantengineering.com, and csemag.com were all affected by the injection from Energetic Bear. Because they're geared toward engineers working in the critical infrastructure sector and thus prime targets for this watering hole attack, the odds are that CFE Media's other websites were affected. In fact, CFE Media has at least six confirmed brands that publish news and information:

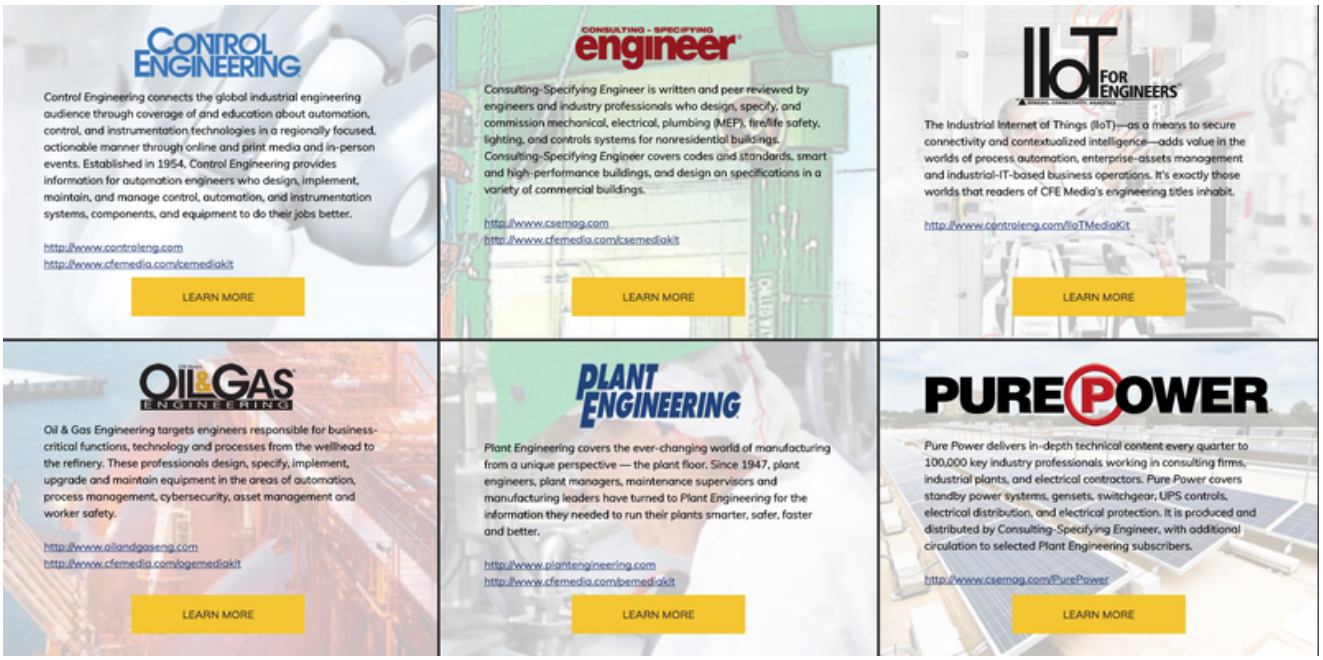


Fig-11 Brands affected by the Energetic Bear campaign

Because we started seeing Energetic Bear's SMB-harvesting injection at the end of March and our crawl data from the end of January was still clean, RiskIQ has been able to pinpoint the start of the campaign to between the beginning of February and the end March.

Conclusion: Don't Feed the Bear

Over the past few years, supply-chain attacks are becoming more and more prevalent in the attacker's portfolio. JavaScript can be changed and compromised without the knowledge of the site owner, finding its way onto a site when public code was modified downstream. To prevent this, site owners must have an understanding of what belongs to their organization, how it's connected to the rest of their asset inventory, including inventorying all the third-party code running on their web assets so they can avoid being a pawn by operators like Energetic Bear.

Signing up for RiskIQ Community Edition now gives you access to one of the most popular RiskIQ products–Digital Footprint. When you sign up or sign in with your organizational email address, you get a glimpse into your organization's attack surface.

To track the full list of IOCs related to this campaign, visit the RiskIQ Community Public Project.

Subscribe to Our Newsletter

Subscribe to the RiskIQ newsletter to stay up-to-date on our latest content, headlines, research, events, and more.

Base Editor