Cimation

ICS Threat Intelligence

#OpPetrol 2014 Cyber Attacks Against Oil & Gas Industry

48-hour Update

June 18, 2014

2014 #OpPetrol Update

#OpPetrol Attacks

Hackers operating under the #OpPetrol umbrella have broadcasted their intent to attack Oil & Gas corporations on June 20th, 2014.

Hacktivists continue to align themselves to #Anonymous and the Middle East protest group #AnonGh0st in preparation for a series of cyber attacks targeting oil and gas corporations on 20 June 2014. This is an anniversary attack aligning with the 2013 #OpPetrol attacks. The hacktivists continue to use social media and other means to advertise their intentions. Their motivation is outlined in an online manifesto stating their belief that the petroleum resources of Middle East countries are being stolen by the West. Further, they believe the people of the region are being controlled as "robots" by their own governments in this "New World Order."

Past 48-hour Updates

Hacktivists published on social media details concerning the defacement of at least 204 additional public websites, none of which, however, directly tied to the oil and gas or ICS/SCADA industries. Supporters have re-published these details as well as #OpPetrol's manifesto on various social media sites.

Tactics, Techniques, and Procedures (TTPs)

Hackers using the #AnonGh0st alias posted three exploits to an open forum, effectively arming their hacktivist followers. The first is a Facebook brute force cracking Perl script which pairs a very large word list to a known email address in an attempt to gain access to a user's Facebook account. The second Perl script attacks a Joomla SQL injection exploit for which a patch has already been distributed. The final Perl script is a cPanel user finder. cPanel is a web hosting account management tool used by website hosting services. (Analyst Comment: The 204 websites hacktivists took down on June 16th were almost exclusively hosted on the same service using cPanel.)

An analysis of social media traffic has revealed a distinct command and control network in use for relaying information pertaining to #OpPetrol. Their personas are almost exclusively variations of the name "Anonymous" and are using Twitter as their primary mode of communication.

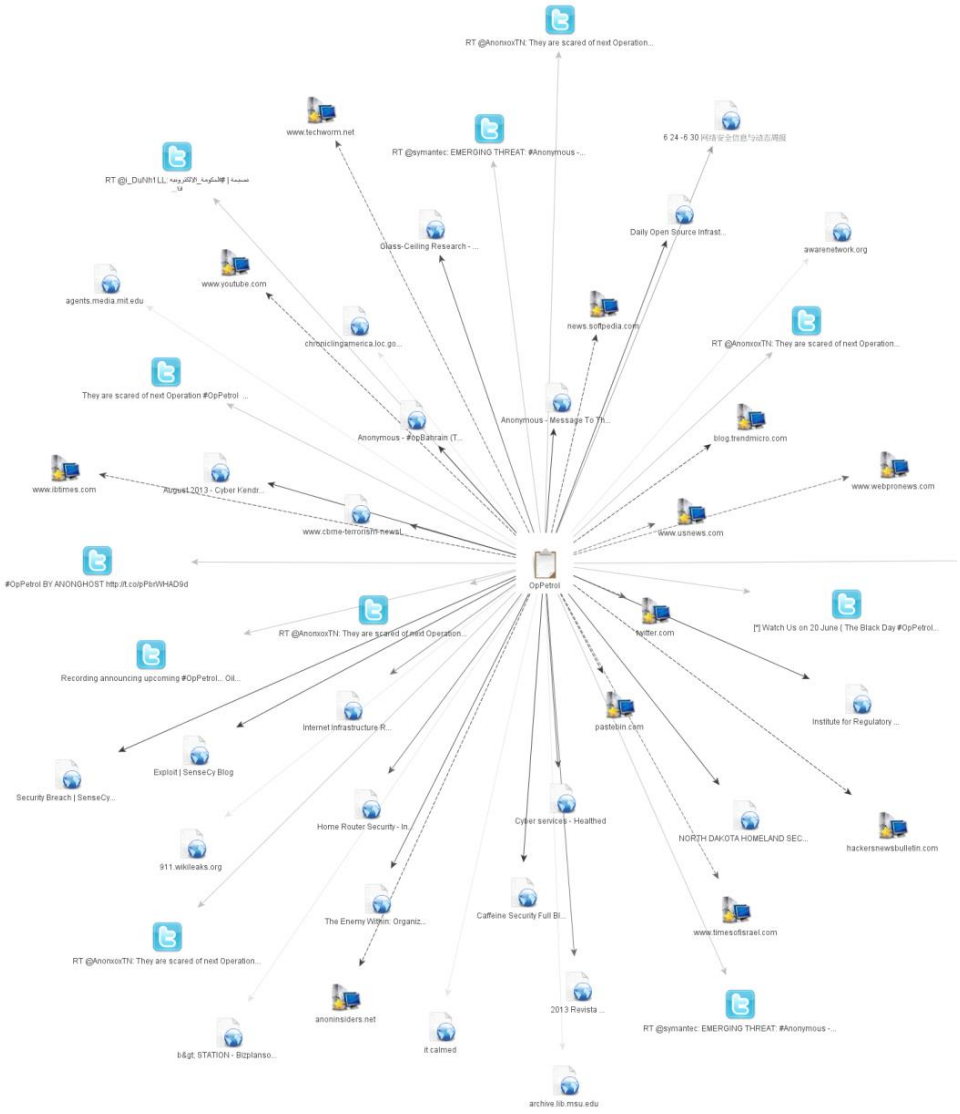

Figure 1. Significant Domains and Nodes Used by #OpPetrol actors.

Analyst Comments

The primary objective of #OpPetrol is to spread the hacktivists' messages to a broad range of consumers. So far, they have not directly attacked oil and gas industry or ICS/SCADA infrastructures or networks. It is in light of this that hacktivists and network defenders have different perspectives and ideas of what defines a "successful hack." #OpPetrol participants have already successfully defaced over 400 public-facing websites. Have they touched a single ICS/SCADA asset? Have they stolen any intellectual property from an oil company? Have they taken control of a pipeline? No….and they may not. It is possible then for both the hacktivists and the network defenders to claim "victory."

Another thing to consider is that dates are incredibly important when analyzing threat actor activity; therefore, it's just as important for cyber security analysts to understand why those dates are important. Cybercriminals who are motivated by financial gain are active during the peak consumer spending periods, especially between November and December of each year. Terrorists have anniversary dates that are incredibly important in their activity planning, and history has shown time and time again that terrorists like to take action to commemorate events that are important to their causes. Financial Service organizations know exactly when to expect attacks against consumers, whether large or small,

and other sectors need to start changing their defensive postures based on cyclic attack cycles. Most hacktivist activity cycles around real world events so that they can get their messages out to broad audiences that are interested in current events. The hacktivist activity associated with the World Cup is a prime example. Other times, hacktivist activity repeats on similar dates to ensure the most effective dissemination of their messages to the broadest group of people.

2014 Targets

See a more exhaustive list of targets at Symantec's Emerging Security blog.

United States of America	Israel	Italy	Germany
Canada	Saudi Arabia (Govt Sites Only)	France	Kuwait (Govt Sites Only)
England (United Kingdom)	Peoples Republic of China	Russia	Qatar (Govt Sites Only)

Next Steps

Symantec has published some very basic risk mitigation techniques in response to the upcoming attacks, but they are typical "defense-in-depth" suggestions since the exact tools had not been published as of the date that Symantec's blog was published. Cimation's Vulnerability Research team will explore in-depth response options as tactics, techniques, and procedures unfold. Cimation's ICS Threat Intelligence team will continue to monitor the threat actors, and will continue to report strategic and tactical intelligence about OpPetrol, the threat actor motivations, intent, capabilities, and methodologies. Vigilance is key, and we will continue to monitor our proprietary Open Source Intelligence streams to provide our clients and partners with the most up to date information on this operation.

For more information on ICS Threat Intelligence & Cyber Security Services, contact ICSCyberIntel@cimation.com.

Click here to register for regular updates from Cimation's ICS Threat Intelligence team straight to your inbox.