Hacker Group Creates Network of Fake LinkedIn Profiles

Sw secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Wednesday, October 7, 2015 *By: Dell SecureWorks Counter Threat Unit™ Threat Intelligence*

- **Author:** Dell SecureWorks Counter Threat Unit™ Threat Intelligence
- **Date:** 07 October 2015

Summary

While tracking a suspected Iran-based threat group known as Threat Group-2889[1] (TG-2889), Dell SecureWorks Counter Threat Unit™ (CTU) researchers uncovered a network of fake LinkedIn profiles. These convincing profiles form a self-referenced network of seemingly established LinkedIn users. CTU researchers assess with high confidence the purpose of this network is to target potential victims through social engineering. Most of the legitimate LinkedIn accounts associated with the fake accounts belong to individuals in the Middle East, and CTU researchers assess with medium confidence that these individuals are likely targets of TG-2889.

Fake LinkedIn accounts

The 25 fake LinkedIn accounts identified by CTU researchers fall into two categories: fully developed personas (Leader) and supporting personas (Supporter). The table in the Appendix lists details associated with the accounts. The level of detail in the profiles suggests that the threat actors invested substantial time and effort into creating and maintaining these personas. The photos used in the fake accounts are likely of innocent individuals who have no connection to TG-2889 activity.

Leader personas

Profiles for Leader personas include full educational history, current and previous job descriptions, and, sometimes, vocational qualifications and LinkedIn group memberships. Of the eight Leader personas identified by CTU researchers, six have more than 500 connections (see Figure 1).

Timothy Stokes
Recruitment Consultant at Teledyne
Technologies Incorporated

Newbury Park, California | Electrical/Electronic
Manufacturing

Current	Teledyne Technologies Incorporated
Previous	ExxonMobil
Education	University of California, San Diego

500+
connections

Join LinkedIn and access Timothy's full profile. It's free!

As a LinkedIn member, you'll join 300 million other professionals who are sharing connections, ideas, and opportunities.

- See who you know in common
- Get introduced
- Contact **Timothy** directly

View Timothy's Full Profile

Summary

I assist in selecting the best-qualified candidates during open hiring. I am involved with screening applications, interviewing candidates and checking references. Our contracts involve the recruitment and secondment of skilled engineers, technicians and managers to client facilities on a domestic or international basis to support major engineering, construction, installation and ongoing operations activities. Teledyne Technologies Inc. owns a globally focused operation, active in over 40 locations, driven by a professional and talented team of people, dedicated to achieving excellence.

Experience

Recruitment Consultant
Teledyne Technologies Incorporated
March 2012 – Present (3 years 5 months) | Thousand Oaks

- Remarkable experience in Recruitment Consultancy
- Project based recruitment, candidate screening & referral networking for both local and emerging
- Ability to identify and successfully qualify candidates
- Familiarity with payroll procedures and taxation issues relevant to contractors
- Good understanding of Consultants contracts and terms and conditions
- Amazing ability to manage independently

Figure 1. Example Leader LinkedIn profile created by TG-2889. (Source: Dell SecureWorks)

The results of open-source research conducted by CTU researchers provided compelling evidence that the Leader profiles were fraudulent:

- One of the profile photographs is linked to multiple identities across numerous websites, including adult sites.
- The summary section in one profile is identical to the summary in a legitimate LinkedIn profile, and the employment history matches a sample résumé downloaded from a recruitment website.
- In another profile, a job description was copied from genuine Teledyne and ExxonMobil job advertisements.
- The job description in yet another profile (see Figure 2) was copied from a legitimate job posting from a Malaysian bank (see Figure 3).

Experience

Research and Development Manager
Teledyne Technologies Incorporated
March 2009 – Present (6 years 5 months) | United States

• Responsible for developing, optimizing and improving products, performances and technologies
• Incorporates relevant design expertise and experience in projects in line with
brand/product strategy
• Encourages creativity in R&D teams
• Actively searches for best-in-class technologies among competitors and develops
innovation road-map
• Cooperates closely with product managers to assure customer focus and target
costing; co-develops product road-maps
• Close collaboration with sales, purchasing, operations and marketing
• Executing necessary tests and analyses

Figure 2. Job description from Leader persona profile. (Source: Dell SecureWorks)

Research And Development Manager
RHB Banking Group
Kuala Lumpur
Login to view salary

Responsibilities:

- Responsible for developing products and driving innovations according to e-Banking product roadmap.
- Assures competitiveness and innovation of products and processes from a technological and user experience stand point on both online banking and mobile banking platform.
- Ensures and consolidates that the growth of the technical "know-how" within the working group is shared and constantly increasing.
- Applies all relevant regulations/norms/standards.
- Leads development projects for locally and regionally including co-development with regional offices.
- Incorporates relevant design expertise and experience in projects in line with brand/product strategy.
- Encourages creativity in R&D teams.
- Actively searches for best-in-class technologies among competitors and develops innovation roadmap.
- Cooperates closely with other business unit managers to assure customer focus and to co-develops product roadmaps.

*Figure 3. Malaysian bank job posting matching a job description associated with a fake Leader LinkedIn profile.
(Source: Dell SecureWorks)*

Five of the Leader personas purport to work for Teledyne, an American industrial conglomerate. In addition, one claims to work for Doosan (an industrial conglomerate based in South Korea), one for Northrop Grumman (a U.S. aerospace and defense company), and one for Petrochemical Industries Co., (a Kuwaiti petrochemical manufacturing company).

Supporter personas

Profiles for Supporter personas are far less developed than for Leader personas. They all use the same basic template with one simple job description, and they all have five connections (see Figure 4). Profile photographs for three of the Supporter personas appear elsewhere on the Internet, where they are associated with different, seemingly legitimate, identities. As with the Leader profiles, open-source research indicates that the Supporter profiles are also fake.

Figure 4. Example Supporter LinkedIn profile created by TG-2889. (Source: Dell SecureWorks)

Building credibility via endorsements

The purpose of the Supporter personas appears to be to provide LinkedIn skills endorsements for Leader personas, likely to add legitimacy to the Leader personas. As shown in Figure 5, most of the Supporter accounts identified by CTU researchers have endorsed skills listed on the profiles of the Leader personas. Although unable to view Leader personas' LinkedIn connections, CTU researchers suspect the threat actors use the Supporter accounts to provide the Leader profiles with an established network, which also enhances credibility.
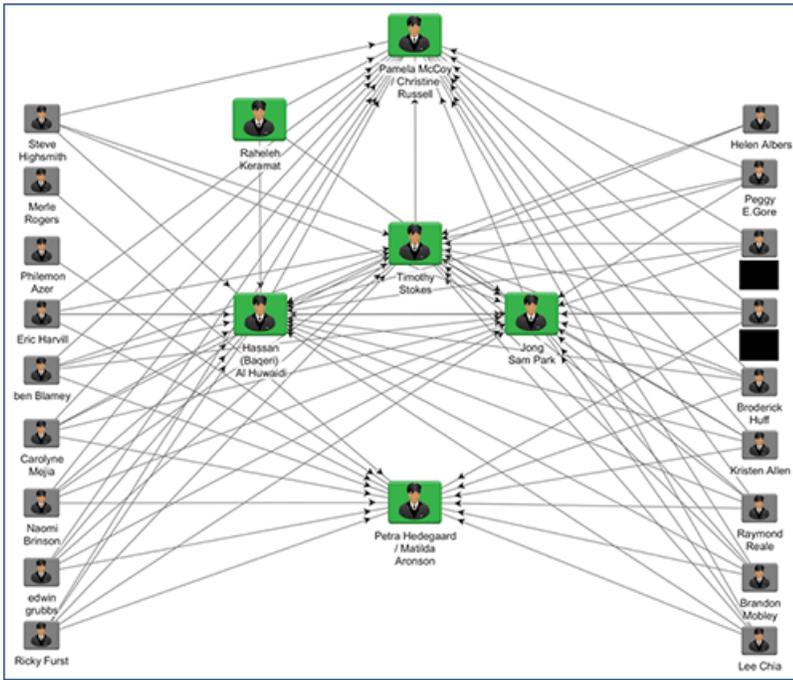
Figure 5. TG-2889 uses Supporter accounts (gray) to endorse the skills of Leader personas (green). (Source: Dell SecureWorks)

Novel technique

Although CTU researchers identified eight Leader profiles, two appear to be duplicates that have different identities associated with the same account. While CTU researchers were analyzing the profiles, the threat actors altered two of the Leader LinkedIn accounts. The original profile name and photograph were replaced with a new identity, and the current job was updated: in one case replacing Teledyne with Northrup Grumman (see Figure 6) and in the second replacing Teledyne with Airbus Group.
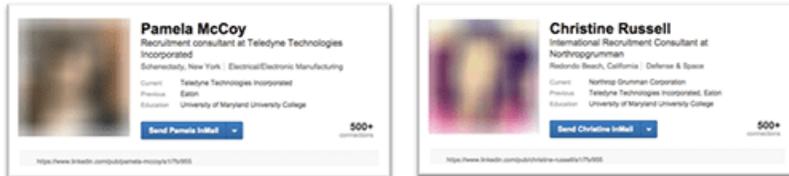

Figure 6. LinkedIn screenshots showing replacement of original Pamela McCoy persona with Christine Russell. The alphanumerical LinkedIn ID, a1/7b/955, remains the same. (Source: Dell SecureWorks)

Changing personas associated with existing profiles was a clever exploitation of LinkedIn functionality because the new identities inherit the network and endorsements from the previous identity. These attributes immediately make the new personas appear established and credible, and the transition may prevent the original personas from being overexposed.

Targeting LinkedIn users

Creating a network of seemingly genuine and established LinkedIn personas helps TG-2889 identify and research potential victims. The threat actors can establish a relationship with targets by contacting them directly, or by contacting one of the target's connections. It may be easier to establish a direct relationship if one of the fake personas is already in the target's LinkedIn network.

Five of the Leader personas claim to be recruitment consultants, which would provide a pretext for contacting targets. TG-2889 likely uses spearphishing or malicious websites to compromise victims, and established trust relationships significantly increase the likelihood of these tactics being successful.

Targets

Seemingly legitimate LinkedIn users have also endorsed Leader personas. Endorsements are granted by connections, indicating that these legitimate users are part of the Leader personas' networks. Therefore, they are likely TG-2889 targets. Examination of the profiles associated with the endorsements revealed 204 potential TG-2889 targets. As shown in Figure 7, most are based in the Middle East.
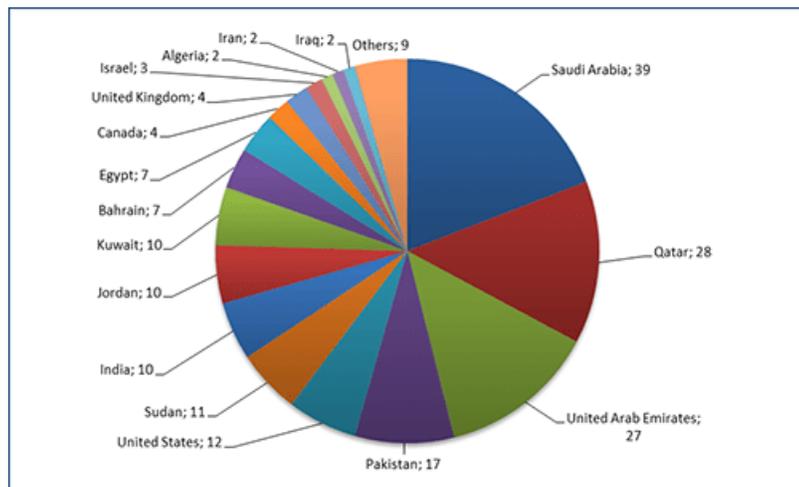

Figure 7. Legitimate endorsers of fake TG-2889 LinkedIn accounts by country. (Source: Dell SecureWorks)

A quarter of the targets work in the telecommunications vertical; Middle Eastern and North African mobile telephony suppliers feature heavily. A focus on these types of targets may indicate that TG-2889 is interested in acquiring data held by these organizations or gaining access to the services they operate. A significant minority of identified targets work for Middle Eastern governments and for defense organizations based in the Middle East and South Asia.

Attribution

Based on strong circumstantial evidence, CTU researchers assess that TG-2889 is linked to the activity that Cylance described in its December 2014 Operation CLEAVER report. The report documented threat actors using malware disguised as a résumé application that appeared to allow résumés to be submitted to the industrial conglomerate Teledyne. Cylance reported the use of the following domains, which reference companies associated with many of the fake LinkedIn profiles identified by CTU researchers:

- Teledyne-Jobs.com
- Doosan-Job.com
- NorthropGrumman.net

Cylance attributed the Operation CLEAVER activity to a threat group operating at least in part out of Iran. CTU researchers have not uncovered any intelligence that contradicts this assessment. Furthermore, the strong focus suggested by the endorsement analysis on targets from Arab states in the Middle East and North Africa (MENA) region is in line with the expected targeting behavior of a threat group operating out of Iran.

Ongoing threat

Updates to profile content such as employment history suggest that TG-2889 regularly maintains these fake profiles. The persona changes and job alterations could suggest preparations for a new campaign, and the decision to reference Northrup Grumman and Airbus Group may indicate that the threat actors plan to target the aerospace vertical.

It is likely that TG-2889 maintains personas that have not yet been identified, and that other threat groups also use this tactic. CTU researchers advise organizations to educate their users of the specific and general risks:

- Avoid contact with <u>known</u> fake personas.
- Only connect to personas belonging to individuals they know and trust.
- Adopt a position of sensible caution when engaging with members of colleagues' or friends' networks that they have not verified outside of LinkedIn.
- When evaluating employment offers originating from LinkedIn, seek confirmation that the individual is legitimate by directly contacting the individual's purported employer.

Organizations may want to consider policing abuse of their brand on LinkedIn and other social media sites. If an organization discovers that a LinkedIn persona is fraudulently claiming an association with the company, it should contact LinkedIn. Creating false identities and misrepresenting an association with an organization is a breach of LinkedIn's terms and conditions.

<u>Appendix</u> — Fake LinkedIn personas created by TG-2889

Table 1 lists details associated with Leader and Supporter personas created by TG-2889. The pairs shaded in dark gray are different identities associated with the same LinkedIn account. The only difference in the profile links of the shared accounts is the persona name.

Type	Name and profile link	Role	Country	Connections	Company
Leader	Jon Sam Park https://www.linkedin.com/pub/jong-sam-park/a0/a46/3	Network Administrator	Korea	500	Doosan
Leader	Pamela McCoy https://www.linkedin.com/pub/pamela-mccoy/a1/7b/955	Recruitment Consultant	United States	500	Teledyne Technologies Incorporated
Leader	Christine Russell https://www.linkedin.com/pub/christine-russell/a1/7b/955	International Recruitment Consultant	United States	500	Northrop Grumman
Leader	Timothy Stokes https://www.linkedin.com/pub/timothy-stokes/a0/a75/b46	Recruitment Consultant	United States	500	Teledyne Technologies Incorporated
Leader	Matilda Aronson https://kr.linkedin.com/pub/matilda-aronson/a1/4a5/227	Recruitment Consultant	Korea	500	Teledyne Technologies Incorporated
Leader	Petra Hedegaard https://kr.linkedin.com/pub/petra-hedegaard/a1/4a5/227	Recruitment Consultant	Korea	500	Airbus Group
Leader	Hassan (Baqeri) Al Huwaidi https://www.linkedin.com/in/hbaqeri	Research and Development Manager	United States	275	Teledyne Technologies Incorporated

Leader	Raheleh Keramat https://www.linkedin.com/pub/raheleh-keramat/99/751/4b	IT Infrastructure Manager	Kuwait	46	Petrochemical Industries Co.
Supporter	Ben Blamey https://uk.linkedin.com/pub/ben-blamey/a2/503/a79	Senior Electronics Project Manager	United Kingdom	5	General Motors
Supporter	Brandon Mobley https://uk.linkedin.com/pub/brandon-mobley/a2/45b/4b	Senior Electronics Design Engineer	United Kingdom	5	General Motors
Supporter	Broderick Huff https://www.linkedin.com/pub/broderick-huff/a1/a50/84	IT Technical and Security Manager	United States	5	Teledyne Technologies Incorporated
Supporter	Carolyne Mejia https://uk.linkedin.com/pub/carolyne-mejia/a1/443/17	IT Support Analyst	United Kingdom	5	Teledyne Technologies Incorporated
Supporter	Edwin Grubbs https://www.linkedin.com/pub/pamela-mccoy/a1/7b/955	IT Recruitment Consultant	United Kingdom	5	Teledyne Technologies Incorporated
Supporter	Eric Harvill https://uk.linkedin.com/pub/eric-harvill/a2/5a5/77b	Electronics Development Engineer	United Kingdom	5	General Motors
Supporter	Helen Albers https://uk.linkedin.com/pub/helen-albers/a2/73b/6b7	Electronics Hardware Engineer	United Kingdom	5	Teledyne Technologies Incorporated
Supporter	Kristen Allen https://www.linkedin.com/pub/kristen-allen/a1/a55/8b4	IT Solutions Manager	United States	5	Teledyne Technologies Incorporated
Supporter	Lee Chia https://www.linkedin.com/pub/lee-chia/a2/506/485	Hardware Design Engineer / Electronics Design	Korea	5	Doosan
Supporter	******* https://www.linkedin.com/pub/*******/a2/600/940	Quality Manager	United Kingdom	5	*******
Supporter	Merle Rogers https://uk.linkedin.com/pub/merle-rogers/a2/378/30b	IT Service Desk Engineer / Support / Windows / Mac OS / Linux	United Kingdom	5	Doosan
Supporter	Naomi Brinson https://www.linkedin.com/pub/naomi-brinson/a2/5b9/23a	Principal Electronics Systems Engineer - DFM, NPI	United Kingdom	5	Unilever
Supporter	Peggy Gore https://uk.linkedin.com/pub/peggy-e-gore/a1/b60/a8b	Head of IT Services and Operations	United Kingdom	5	Doosan

Supporter	Raymond Reale https://uk.linkedin.com/pub/raymond-reale/a1/497/689	Project and Program Manager Assistant at Teledyne Technologies Incorporated	United Kingdom	5	Teledyne Technologies Incorporated
Supporter	Ricky Furst https://www.linkedin.com/pub/ricky-furst/a1/967/84a	IT Manager at Teledyne Technologies Incorporated	United States	5	Teledyne Technologies Incorporated
Supporter	******* https://www.linkedin.com/pub*******a67	IT Support Analyst at Teledyne Technologies Incorporated	United States	5	Teledyne Technologies Incorporated
Supporter	Steve Highsmith https://uk.linkedin.com/pub/steve-highsmith/a1/b57/4ab	IT Operations Manager at Doosan	United Kingdom	5	Doosan

Table 1. Fake LinkedIn personas. Some potentially sensitive information has been redacted.

Endnote

[1] The Dell SecureWorks Counter Threat Unit(TM) (CTU) research team tracks threat groups by assigning them four-digit randomized numbers (2889 in this case), and compiles information from external sources and from first-hand incident response observations.