DeepSight™ INTELLIGENCE

FORMER SENIOR U.S. OFFICIAL'S FINANCIAL FIRM TARGETED BY IRANIAN CYBER ESPIONAGE

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE REPORT | SYMC - 300242 | V.1
30 JUL 2015 GMT

LEGAL NOTICE

SYMANTEC PROPRIETARY & CONFIDENTIAL - PERMITTED USE ONLY

Symantec assigns a high, medium, or low degree of confidence to assessments within its DeepSight™ Intelligence Portal Managed Adversary and Threat Intelligence (MATI) products. Confidence levels are determined against a three-point spectrum of source validity: variety and non-conflictive disparity of original sources, quality of source reporting, and reliability of source reporting. Confidence levels may be increased based on independent corroboration of information. High confidence generally suggests a solid judgment can be made, though such a judgment carries the risk of being wrong. Low confidence generally suggests tenuous inferences can be made, though information used to do so may have been questionable, fragmented, or singular.

Information Cut-Off Date: 28 Jul 2015 GMT

Former Senior U.S. Official's Financial Firm Targeted by Iranian Cyber Espionage

DeepSight™ Intelligence | Intelligence Report | SYMC - 300242 | V.1 | 30 Jul 2015 GMT

KEY FINDINGS

ATG9 targeted the email address at a US-based financial organization that belonged to a former senior US government official on 1 July 2015. ATG9 actors likely leveraged open source intelligence (OSINT) to devise the email targeting.

The lure document used in the email contains multiple clear links to previous ATG9 spearphishing lure documents but was likely unsuccessful due to a programming error.

This operation highlighted ATG9 targeting of a second financial industry executive in July 2015. It is likely that ATG9 is targeting financial industry executives due to their awareness and perceived ability to influence policies related to the Iran nuclear agreement.

EXECUTIVE SUMMARY

A former senior US government official, who is now a financial industry executive, was targeted by an ATG9 cyber operation on 1 July 2015. It is almost certain that the group conducted extensive pre-operation open-source research on this target due to their extensive knowledge of the target's role in international politics. While the ATG9 group's research of the target appears to be ample, errors in the lure file demonstrate that the group lacks operational procedures that include testing the attachments prior to their use in cyber operations.

This activity is the second instance of ATG9 targeting a pro-Israel financial industry executive using Iranian nuclear agreement-themed lures in July 2015. It is possible that ATG9 is targeting executives, who can influence their industry's policy, to gain insight into their sentiments regarding the Iranian nuclear agreement. DeepSight Intelligence refers to the Rocket Kitten group as Advanced Threat Group 9 (ATG9).

DETAILS

On 1 July 2015, ATG9 (a.k.a. Rocket Kitten) used a spearphishing email with the subject line “Chance to reach a deal with Iran?” to target an executive-level employee at a US financial organization (see Figure 1). The individual is a former senior US government official who held a high-visibility leadership role within a large US government agency. In his previous government role, the target publicly expressed strong support for Israel, which is similar to a previously reported ATG9 target.[1]

Figure 1. Spearphishing email that targeted the former senior US government official

Target Selection and the Use of Available OSINT

ATG9 actors displayed clear indications that they collected OSINT about the target and his previous relationships to construct a believable spearphishing email. Given the high-visibility role within the US government previously held by the target, there was an abundance of valuable targeting information available to ATG9 actors. The target has made numerous public, decisively pro-Israel comments and has also called for a strong multinational effort to prevent Iran from acquiring nuclear weapons.

The target’s email address followed a pattern that would have made it difficult for ATG9 actors to guess. The email address used the first initial of the target’s first name and three numbers (e.g., a127@company.com). Despite the absence of the employee’s name in the email address, the salutation in the email body referenced the target by full first name. DeepSight Intelligence’s research on the target revealed a document from 2013 that published his name and email address.

This operation impersonated former Israeli General Amos Yadlin as the sender of the email using the email address of gen.yadlin[@]walla.co.il. Yadlin now serves as the director of the Institute for National Security Studies at Tel Aviv University. The targeted individual has worked with Yadlin on matters involving Middle Eastern conflict and politics. Additionally, Yadlin has been a prominent source of public commentary on the Israeli nuclear deal and Iran’s nuclear initiatives for over 10 years.

ATG9 Lure File: “Chance to reach a deal with Iran.xlsb”

The Microsoft Excel file attachment named “Chance to reach a deal with Iran.xlsb” (MD5:

2c28bad7cf0b5344d2df6c8fdb15338b) was the same lure file linked to ATG9 in previous DeepSight Intelligence reporting against a UK-based financial industry executive; in that attack the file was named “iran-deal-text.xlsb”[1] As previously reported and in this activity, the metadata of the file contained values that were common across a number of ATG9 lure files (see Figure 2). [2][3]

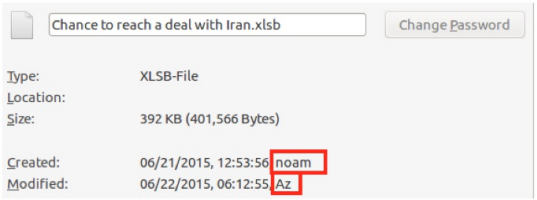

Figure 2. Metadata of the file “Chance to reach a deal with Iran.xlsb” (MD5: 2C28BAD7CF0B5344D2DF6C8FDB15338B)

Analysis of the lure file revealed the presence of a programming error in the macro within the ATG9 lure file. This error prevented the file from executing and compromising the targeted host. Previous ATG9 lure files have contained the same or similar errors with the same result of failure. These mistakes highlight the group’s lack of robust testing prior to launching an operation.

[1] See the DeepSight Intelligence report *Financial Organizations Targeted by ATG9 Based on Connections with Iran Nuclear Agreement* (SYMC-300237), 25 July 2015.

[2] See the DeepSight Intelligence report *Rocket Kitten Cyber Activity Predominantly Targeting Israeli Entities in September 2014-January 2015* (SYMC-300101), 19 February 2015.

[3] See the DeepSight Intelligence report *Lure Document in Hebrew with Academic Theme Linked to Iran-Based Rocket Kitten Cyber Espionage Group* (SYMC-300198), 5 June 2015.

OUTLOOK

This ATG9 operation showed continued targeting of financial sector executives involved in international politics. This highly selective targeting suggests an interest in gathering intelligence pertaining to the Iranian nuclear deal, not the normal corporate dealings of their employer. It is highly likely that ATG9 will target other financial industry executives who have had a public opinion on the Iranian nuclear agreement or made pro-Israel statements about international politics. These intelligence gathering initiatives appear clearly aligned with Iranian national interests.

While the group demonstrated adequate OSINT collection to craft a believable targeted email from the available information, other operational shortfalls, including a lack of pre-operational testing of their lure file, resulted in the likely failure of this operation. Coupled with the continued use of the same C&C infrastructure and lure metadata, ATG9 currently lacks the ability to be consistently successful against well-defended targets.

TECHNICAL DETAILS

See the ***Metadata*** tab for the technical details and indicators of compromise related to this report.

METADATA

ACTORS

Name	Facebook Account	Orkut Account	Twitter Account	Pastebin Site	Tumblr Account	Vkon takte Account
ATG9						

CAMPAIGNS

Name	ID	Status
ATG9-CE.0072	CE.0072	Active

EXTRACTED INDICATORS

Indicator	Indicator Related CVE	Indicator Type
84.11.146.62		ip_address
ATG9		actor
Chance to reach a deal with Iran.xlsb		file_name
2c28bad7cf0b5344d2df6c8fdb15338b		file_md5
187a8047793a5d34ae94f353aa1f8634a7471ec49f2723a4827a133d24a5f439		file_sha256
outpu1.exe		file_name
2a6da1fc0c8db87a6c3be6f45f21565e		file_md5
e55f0a03337844c84c41684f75b1be9dfd772ab9f531e2e10f1dc7b0df0584af		file_sha256

FILES

Detection Name	Name	MD5	SHA 256	Malicious
O97M.Dropper	Chance to reach a deal with Iran.xlsb	2c28bad7cf0b5344d2df6c8fdb15338b	187a8047793a5d34ae94f353aa1f8634a7471ec49f2723a4827a133d24a5f439	y
	outpu1.exe	2a6da1fc0c8db87a6c3be6f45f21565e	e55f0a03337844c84c41684f75b1be9dfd772ab9f531e2e10f1dc7b0df0584af	y

TARGET INDUSTRIES

NAICS Code	Name
52	Finance and Insurance
92	Public Administration

SOURCE REGIONS

Region	Asia

Subregion	Southern Asia
Countries	Iran, Islamic Republic Of

TARGET REGIONS

Region	Europe
Subregion	Northern Europe
Countries	United Kingdom

THREAT DOMAINS

Cyber Espionage