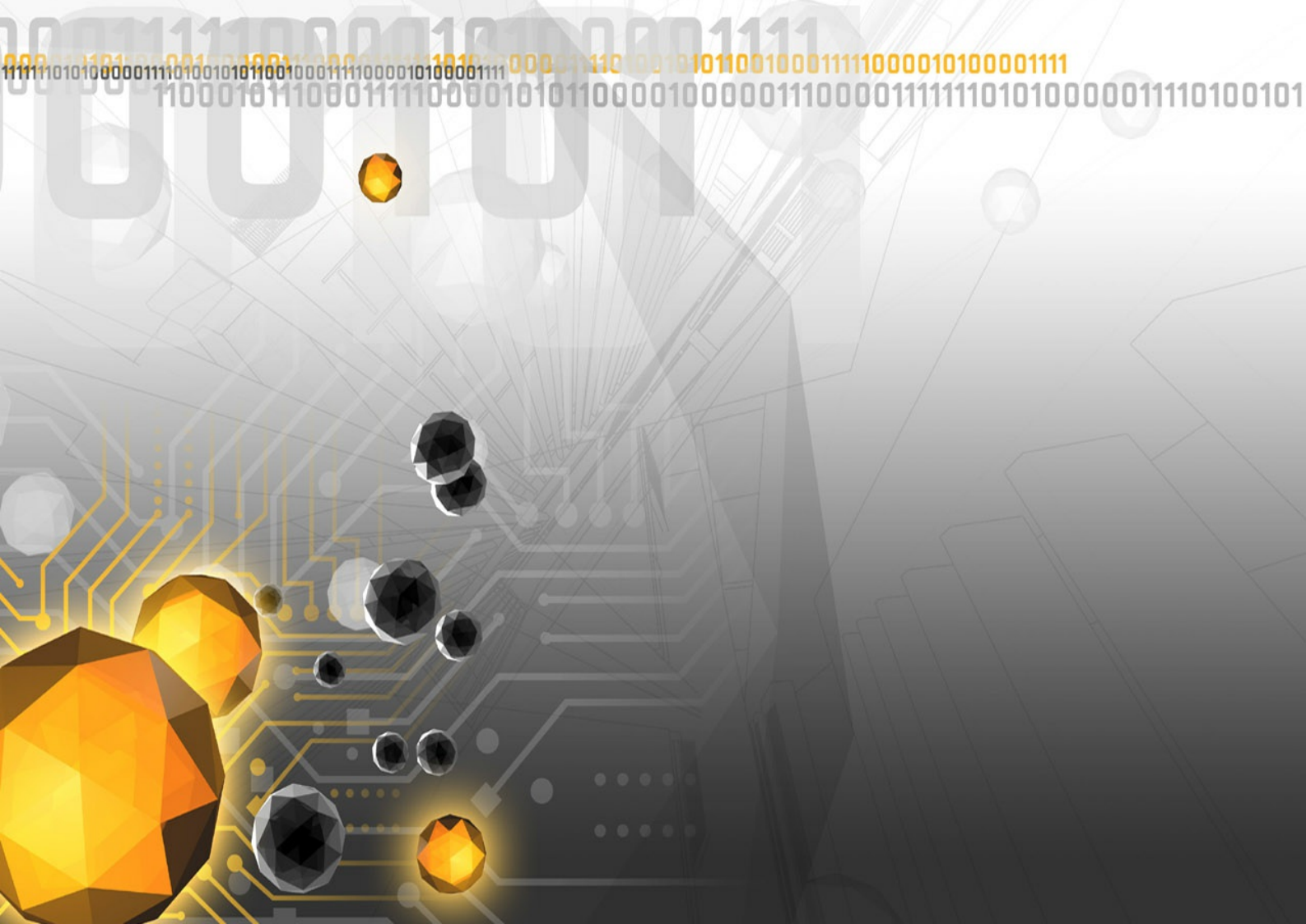
DeepSight™ INTELLIGENCE

PROFILE: ROCKET KITTEN ACTOR WOOL3N.H4T

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE PROFILE | SYMC - 300135 | V.1
13 APR 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: 31 Mar 2015 GMT

Profile: Rocket Kitten Actor Wool3n.H4t

DeepSight™ Intelligence | Intelligence Profile | SYMC - 300135 | V.1 | 13 Apr 2015 GMT

KEY FINDINGS

Symantec has identified that Woolen.H4t, a threat actor previously linked to the operations of suspected Iranian cyber espionage group Rocket Kitten, has been involved with the creation of Microsoft Excel lure files and the CWoolger keylogger.[1] The files containing metadata linked to Wool3n.H4t have been used to target government and academic organizations in Israel and Western Europe since at least April 2014.

Symantec assesses with medium confidence that Wool3n.H4t can develop malware and social engineering lures for use in computer network exploitation, but currently lacks the operational security techniques necessary to conceal identifiable information that links him to the activity. Metadata from the Excel lure files and the CWoolger keylogger contained information that is attributable to the Wool3n.H4t alias.

Symantec assesses with low confidence that the true identity of Wool3n.H4t is Masoud Pourkazemi, a Tehran, Iran-based individual and student at Sadra University with an interest in computer programming. Using a personal blog referencing both aliases Wool3n.H4t and masoud_pk, Symantec identified additional information about the possible name, age, location, interests, and education of Wool3n.H4t.

---

[1] See the Symantec Deepsight Intelligence, Intelligence Report *Newly Identified Infrastructure and Lure Files Associated with Rocket Kitten Cyber Espionage Group* (SYMC-300113) published on 12 March 2015 for more information on the network infrastructure and lure files associated with Rocket Kitten cyber espionage operations.

EXECUTIVE SUMMARY

Symantec has identified the presence of metadata containing the alias Wool3n.H4t in files used during Rocket Kitten cyber operations between 23 April 2014 and 6 January 2015. These files have been used to target government and academic organizations in Israel and Western Europe since at least April 2014. Symantec assesses with medium confidence that this actor, while capable of developing malware and lures for social engineering attempts, currently lacks the operational security techniques necessary to conceal identifiable information linking the Wool3n.H4t moniker to this activity. Due to a 19 March 2015 public report on Wool3n.H4t's role in Rocket Kitten cyber operations, Symantec expects that future development by Wool3n.H4t will apply improved operational security, including the sanitization of metadata and identifiable strings, as well as the obfuscation of clear-text account credentials.

Symantec assesses with low confidence that the true identity of Wool3n.H4t is Masoud Pourkazemi, a Tehran, Iran-based individual and student at Sadra University with an interest in computer programming. Symantec has identified several online accounts linked to the aliases Wool3n.H4t and

masoud_pk, including accounts that revealed additional information about Masoud Pourkazemi's identity such as age, location, interests, and education.

DETAILS

Symantec assesses with medium confidence that Rocket Kitten actor Wool3n.H4t can develop malware and social engineering lures for use in computer network exploitation, but currently lacks the operational security techniques necessary to conceal identifiable information linking the Wool3n.H4t moniker to this activity. The Wool3n.H4t alias has been used in the metadata and an email address contained within the CWoolger keylogger, which included the username and password of the email account woolen.h4t@gmail.com. Furthermore, a Japan-based cyber security company's 19 March 2015 technical report highlighted a debug string that contained a file path linking the Wool3n.H4t alias to the development of the CWoolger keylogger which also included FTP credentials that were in clear text within the binary.

ROCKET KITTEN

Rocket Kitten activity seen as early as April 2014 was publicly reported during a 28 December 2014 technical presentation at a German-based cyber security conference as an, "advanced APT set of campaigns with a twist—off-the-shelf malware that won't shame a nation state." Symantec has previously reported on Rocket Kitten cyber espionage operations, most notably against organizations in the government and academic organizations in Israel and Western Europe.

According to Symantec technical research, as of 2 February 2015 eight Microsoft Excel lure files contained the value Wool3n.H4t in the creator and lastModifiedBy fields (see Figure 1). Metadata values can be changed from within the Microsoft application to be blank or contain a value of the user's choice.

MD5	creator	CreateDate	lastmodifiedby	ModifyDate
08273c8a873c5925ae1563543af3715c	Wool3n.H4t	2014:06:23 05:06:07Z	UK	2014:07:27 09:40:32Z
177ef7faab3688572403730171ffb9c4	Wool3n.H4t	2014:06:23 05:06:07Z	UK	2014:07:15 07:54:32Z
271a5f526a638a9ae712e6a5a64f3106	Wool3n.H4t	2014:06:23 05:06:07Z	aikido1	2014:07:07 05:24:57Z
393bd2fd420eecf2d4ca9d61df75ff0c	Wool3n.H4t	2014:04:26 04:51:37Z	Hoffman	2014:04:28 10:07:52Z
395461588e273fab5734db56fa18051b	Wool3n.H4t	2014:04:23 04:03:01Z	Wool3n.H4t	2014:04:23 06:12:00Z
50d3f1708293f40a2c0c1f151c2c426f	Wool3n.H4t	2014:06:23 05:06:07Z	aikido1	2014:07:02 15:22:55Z
5a009a0d0c5ecaac1407fb32ee1c8172	Wool3n.H4t	2014:06:23 05:06:07Z	UK	2014:07:27 11:57:21Z
5af0cbc18c6f8ed4fd1a3f68961f5452	Wool3n.H4t	2014:04:23 04:03:01Z	Wool3n.H4t	2014:04:23 05:55:46Z

Figure 1. Microsoft Excel lure files that contained Wool3n.H4t in the file's metadata

According to Symantec technical research, as of 2 February 2015 a file named AdobeReader.exe (MD5: 0b0e2c4789b895e8ac44b6ada284aec1) was linked to Rocket Kitten cyber espionage operations by a United States-based cyber security company in a 28 December 2014 technical presentation. The file contained an instance of the SmtpClient class (see Figure 2) that was configured to use the email address woolen.h4t@gmail[.]com and password. (The SmtpClient class allows applications to use the Simple Mail Transfer Protocol (SMTP) to send e-mail).

```
new SmtpClient
{
Host = "smtp.gmail.com",
EnableSsl = true,
Port = 25,
Credentials = new NetworkCredential("woolen.h4t", "W00[redacted]!"
}
```

Figure 2. Function found within file AdobeReader.exe (MD5: 0b0e2c4789b895e8ac44b6ada284aec1); the file contained email credentials for woolen.h4t@gmail.com

According to a 19 March 2015 technical report by a Japan-based cyber security company, as of 31 March 2015 a sample of the CWoolger keylogger contained the following debug string: C:\Users\Wool3n.H4t\Documents\Visual Studio 2010\Projects\C-CPP\CWoolger\Release\CWoolger.pdb. This string links the Windows user name Wool3n.H4t to the development of the CWoolger keylogger. The technical report also noted that this sample contained hard-coded credentials in clear text in the binary for an FTP server used by the keylogger.

Symantec assesses with low confidence that the true identity of Wool3n.H4t is Masoud Pourkazemi, an Iranian male in his mid-20s with an interest in computer programming and a student at Sadra University in Iran. A blog located at wool3nh4t.blog[.]ir contained two entries written on 25 January 2014 that were signed using the name masoud_pk. Using variations of the Wool3n.H4t and masoud_pk aliases, Symantec identified additional online presence, including an Instagram site using the username masoud_pk that listed his name, location, and year of birth as Masoud Pourkazemi, a Tehran, Iran-based male born in 1992. The Facebook profile indicating that he had studied at Sadra University in Iran. Furthermore, the wool3nh4t.blog[.]ir blog contained three links to Bayan, an Iran-based computer programming contest, which indicates masoud_pk's interests align with the software development performed by Wool3n.H4t to support Rocket Kitten cyber operations.

According to a 19 March 2015 technical report by a Japan-based cyber security company, as of 31 March 2015 a blog hosted at wool3nh4t.blog[.]ir contained only two entries, which were both written on 25 January 2014 and signed with the alias masoud_pk. This blog contained four links, outlined below in Figure 3. Three of the four links related to Bayan, an Iran-based computer programming competition.

Link Description	Link URL	Description of Site
انی‌ب شرکت ی‌رم‌یم و‌بل‌اگ (The official blog of the company Bayan)	http://bayan.blog.ir/	An Iran-based programming contest.
انی‌ب صن‌دوق (P.o. box Bayan)	http://bayanbox.ir/	A file sharing website possibly used to support Bayan.
ت‌قل‌ب ه‌ی ع‌ل‌یه اس‌ت‌اد‌ان (Professors against fraud)	http://pap.blog.ir/	A blog for Professors Against Plagiarism.
انی‌ب ی‌ه‌ی‌ن‌و ب‌رن‌ام‌ه‌س‌ابق‌ات (Bayan programming competitions)	http://contest.bayan.ir/	An Iran-based programming contest.

Figure 3. Four links found on blog wool3nh4t.blog[.]ir

According to Symantec research, as of 31 March 2015 the username masoud_pk was used for the online service Instagram (hxxps://instagram[.]com/masoudpourkazemi). On this site, the user listed his location as Tehran, Iran and his birth year as 1992 (see Figure 4). A Facebook profile for Masoud Pourkazemi (Figure 5) used the same photo as the Instagram site in Figure 4 and indicated that he studied at Sadra University in Iran.

Figure 4. Instagram profile for username masoud_pk

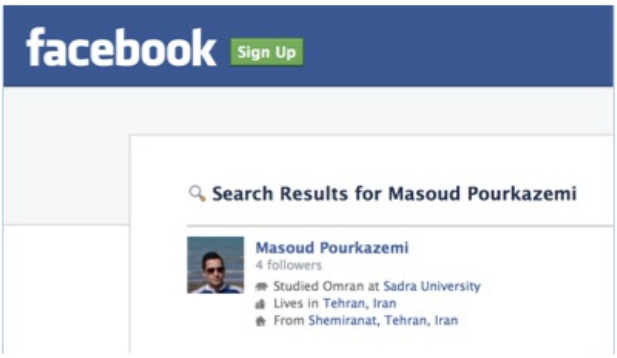


Figure 5. Facebook search results for Masoud Pourkazemi

OUTLOOK

Symantec DeepSight Intelligence previously reported on Wool3n.H4t's involvement in Rocket Kitten cyber espionage activities prior to the Japan-based cyber security company's public report on 19 March 2015 that linked the Wool3n.H4t alias to the operation. Symantec expects public exposure of Wool3n.H4t will result in his use of additional operational security measures such as the sanitization of metadata and the introduction of obfuscation for clear-text account credentials in the CWoolger keylogger and other tools he develops in the next one-to-three months.

TECHNICAL DETAILS

Name: Masoud Pourkazemi

Facebook: http://facebook[.]com/masoud.pourkazemi

Instagram: https://instagram[.]com/masoudpourkazemi

Email: woolen.h4t@gmail[.]com

Blog: wool3nh4t.blog[.]ir

Display Name: masoud_pk

Location: Tehran, Iran

Kik: masoud_pourkazemi

DOB: 1992

METADATA

ACTORS

Name	Facebook Account	Orkut Account	Twitter Account	Pastebin Site	Tumblr Account	Vkon takte Account
Wool3n.H4t	masoud.pourkazemi					

EXTRACTED INDICATORS

Indicator	Indicator Related CVE	Indicator Type
Wool3n.H4t		actor
08273c8a873c5925ae1563543af3715c		file_md5
5c1064dcadafd39b71455031d57ba13cf2dc6d5aa7c493e9d2fdbf963139ea63		file_sha256
177ef7faab3688572403730171ffb9c4		file_md5
a0aca58ca8ec5749b13310bf112d1b4ded6d461bfd8fba92d9e38f8536a39c8d		file_sha256
271a5f526a638a9ae712e6a5a64f3106		file_md5
cde4b40c92c0d23a4aa82f712722e32817440f79676092c3a69cffb56e8aab04		file_sha256
393bd2fd420eecf2d4ca9d61df75ff0c		file_md5
20c940f83c3b8402a7c941e8370684068591c0c9c27061a71641e4a585923937		file_sha256
395461588e273fab5734db56fa18051b		file_md5
01e41fa4b6342d1fc9abb015f3341a8b926a77ceb9bb31b21c4f231cc7324abd		file_sha256
50d3f1708293f40a2c0c1f151c2c426f		file_md5
f1830fdc968b3fc101c53125cc47b6298964b9a218af833093c04bdd0c61036c		file_sha256
5a009a0d0c5ecaac1407fb32ee1c8172		file_md5
9808170e6e84b6ab1f90ec1833220dd83cdf5db08f3dd5f02d5cfa9c828f6633		file_sha256

Indicator	Indicator Related CVE	Indicator Type
5af0cbc18c6f8ed4fd1a3f68961f5452		file_md5
a962fd877c1c4e90095e6f32bc089ee76b141ebd6fee046755d5f316d355139b		file_sha256

FILES

Detection Name	Name	MD5	SHA 256	Malicious
O97M.Dropper		08273c8a873c5925ae1563543af3715c	5c1064dcadafd39b71455031d57ba13cf2dc6d5aa7c493e9d2fdbf963139ea63	y
O97M.Dropper		177ef7faab3688572403730171ffb9c4	a0aca58ca8ec5749b13310bf112d1b4ded6d461bfd8fba92d9e38f8536a39c8d	y
O97M.Dropper		271a5f526a638a9ae712e6a5a64f3106	cde4b40c92c0d23a4aa82f712722e32817440f79676092c3a69cffb56e8aab04	y
O97M.Dropper		393bd2fd420eecf2d4ca9d61df75ff0c	20c940f83c3b8402a7c941e8370684068591c0c9c27061a71641e4a585923937	y
O97M.Dropper		395461588e273fab5734db56fa18051b	01e41fa4b6342d1fc9abb015f3341a8b926a77ceb9bb31b21c4f231cc7324abd	y
O97M.Dropper		50d3f1708293f40a2c0c1f151c2c426f	f1830fdc968b3fc101c53125cc47b6298964b9a218af833093c04bdd0c61036c	y
O97M.Dropper		5a009a0d0c5ecaac1407fb32ee1c8172	9808170e6e84b6ab1f90ec1833220dd83cdf5db08f3dd5f02d5cfa9c828f6633	y
None		5af0cbc18c6f8ed4fd1a3f68961f5452	a962fd877c1c4e90095e6f32bc089ee76b141ebd6fee046755d5f316d355139b	y

TARGET INDUSTRIES

NAICS Code	Name
92	Public Administration
61	Educational services

SOURCE REGIONS

Region	Asia
Subregion	Southern Asia
Countries	Iran, Islamic Republic Of

TARGET REGIONS

Region	Asia
Subregion	Western Asia
Countries	Israel

THREAT DOMAINS

Cyber Espionage