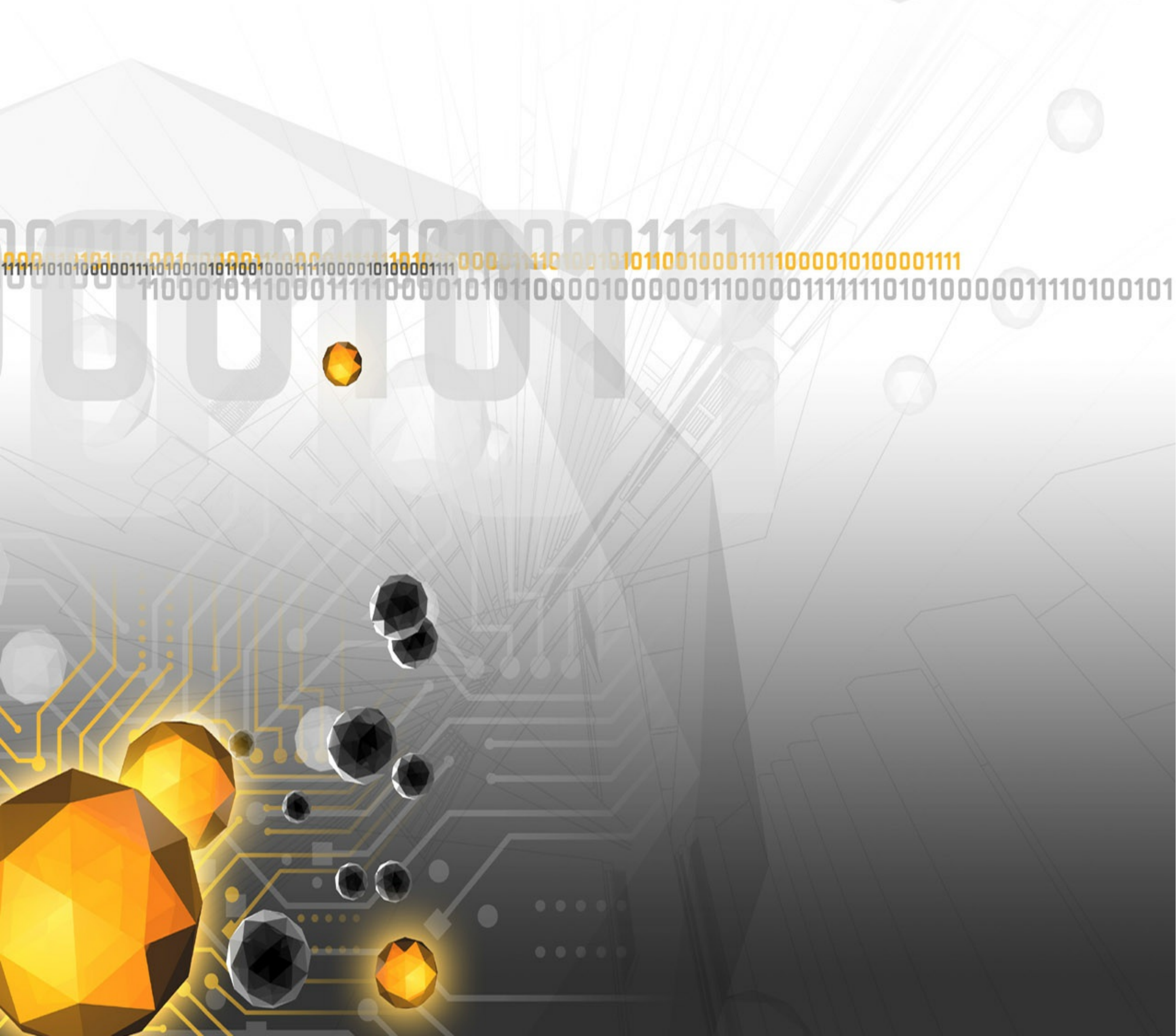
ROCKET KITTEN OPERATIONS CONTINUE AGAINST MIDDLE EAST TARGETS IN JUNE 2015

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE REPORT | SYMC - 300218 | V.1
01 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: 27 Jun 2015 GMT

Rocket Kitten Operations Continue Against Middle East Targets in June 2015

DeepSight™ Intelligence | Intelligence Report | SYMC - 300218 | V.1 | 01 Jul 2015 GMT

KEY FINDINGS

Rocket Kitten, a cyber espionage adversary group who has conducted operations against Israel, is now using their infrastructure to also target victims in Jordan.

A dropper associated with Rocket Kitten was observed with a hard-coded IP address that is capable of requesting additional instructions from the command-and-control (C&C) server.

Rocket Kitten attempted to open a reverse shell using the Metasploit Framework's Meterpreter from the same hard-coded IP address identified and used as C&C infrastructure in previous Rocket Kitten activity.

EXECUTIVE SUMMARY

Rocket Kitten, a probable Iran-based cyber espionage group, continued its targeting of Middle East-based entities between late-May and mid-June 2015. Infrastructure previously attributed to Rocket Kitten was used in operations against Israell-based targets; however, in the recent wave of attacks, targeting has expanded to include victims located in Jordan. In previous and recent activity, a dropper was used to provide the initial infection vector delivering malware and to introduce post-compromise tools into the target's environment. Additionally the commodity penetration-testing framework Metasploit was used in the recent attacks to target the victim's organizations.

DETAILS

The activity included the use of a low-complexity dropper designed to communicate with a hard-coded C&C IP address previously associated with Rocket Kitten. DeepSight Intelligence documented Rocket Kitten activity involving the hard-coded IP address in a previous report detailing operations against Israel-based victims.[1].

From late-May through mid-June 2015, Rocket Kitten was observed using the IP address 84[.]11.146.62 as C&C infrastructure in activity against victims in Israel and Jordan. The activity included the use of a low-complexity dropper designed to communicate with a hard-coded C&C IP address previously associated with Rocket Kitten. DeepSight Intelligence documented Rocket Kitten activity involving the hard-coded IP address in a previous report detailing operations against Israel-based academic institutions. However, in this wave of attacks, targeting was expanded to include Jordan-based targets in addition to the previously reported attacks against Israel.

DeepSight Intelligence observed the use of four malware samples as part of this activity (see Figure 1). Each of the samples was linked to Rocket Kitten operations through the use of the hard-coded IP address 84[.]11.146.62. These samples were droppers designed to check for the presence of a debugger and, if none is detected, contact the hard-coded C&C IP address 84[.]11.146.62. No additional stages of malware were observed; however, it is almost certain that these samples were leveraged by the Rocket Kitten group to introduce more comprehensive tools into the victims' environments.

Date(s) Observed	MD5	Countries Targeted
27 May 2015	55FF220E38556FF902528AC984FC72DC	Jordan
16-17 June 2015	33AE2B0886A53CFD74FDF0CEB6A06986	Israel
16-18 June 2015	CF2591ABC8D274F44113A720B69D75BE	Israel
Unknown	2CB23916CA60A63A67D974F4DDEB2A11	Unknown

Figure 1. Samples containing the hard-coded C&C IP address 84[.]11.146.62

In at least one confirmed instance, the Rocket Kitten operators attempted to open a reverse shell using the Metasploit Framework's Meterpreter from the same hard-coded IP address identified and used as C&C infrastructure in previous Rocket Kitten activity. While the attack was unsuccessful against the target, it demonstrates that Rocket Kitten is likely using the Metasploit Framework as part of their operation to exploit targets and to possibly maintain persistent access.

[1] See 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

Given the limited capabilities of the dropper and the group's traditional intent to gather sensitive information from targeting organizations, it is almost certain that additional information stealing malware would be introduced into the victim's system during the next stage of infection.

Rocket Kitten's use of Metasploit's Meterpreter is a likely indication that the group is attempting to further their operations using traditional penetration testing tools. Organizations should remain highly diligent with their vulnerability patching levels, especially when publicly accessible tools such as Metasploit deliver modules for vulnerabilities that adversary groups can exploit.

This activity highlights the continuation of Rocket Kitten's Middle East-focused targeting using a combination of basic malware implants and commodity tools. Based on the group's apparent preference to compromise targets using spearphishing emails, it is probable that the initial vector used to introduce this dropper was social engineering written in the language of the intended recipient—Hebrew or Arabic. As a result of the group relying heavily on user interaction for network compromise, it is critical for organizations to implement social engineering and spearphishing awareness training programs to prevent the success of Rocket Kitten and other adversary groups using similar tactics.

TECHNICAL DETAILS

See the ***Metadata*** tab for additional technical details related to this report.

METADATA

CAMPAIGNS

Name	ID	Status
Rocket Kitten	CE.0026	Active

EXTRACTED INDICATORS

Indicator	Indicator Related CVE	Indicator Type
55FF220E38556FF902528AC984FC72DC		file_md5
072a43123e755ad1bdd159488a85a353227ec51f273c4f79c26ff7e4656c0ef4		file_sha256
CF2591ABC8D274F44113A720B69D75BE		file_md5
63fd73e99ffa235dcb7eebc3a6e48e73d02a5721280de24f6cb9c572c2d4ca03		file_sha256
33AE2B0886A53CFD74FDF0CEB6A06986		file_md5
5d30a201c013bccbc61dc21821770af09fe76c59a80b87f0023aaad02cdee58e		file_sha256
2CB23916CA60A63A67D974F4DDEB2A11		file_md5
842e8c6b7b7c3d5e2ce35d04c01af35796b702e81174bc62dabaecd74522b9df		file_sha256
84.11.146.62		ip_address

FILES

Detection Name	Name	MD5	SHA 256	Malicious
		55FF220E38556FF902528AC984FC72DC	072a43123e755ad1bdd159488a85a353227ec51f273c4f79c26ff7e4656c0ef4	Y
		CF2591ABC8D274F44113A720B69D75BE	63fd73e99ffa235dcb7eebc3a6e48e73d02a5721280de24f6cb9c572c2d4ca03	Y
		33AE2B0886A53CFD74FDF0CEB6A06986	5d30a201c013bccbc61dc21821770af09fe76c59a80b87f0023aaad02cdee58e	Y
None		2CB23916CA60A63A67D974F4DDEB2A11	842e8c6b7b7c3d5e2ce35d04c01af35796b702e81174bc62dabaecd74522b9df	y

TARGET INDUSTRIES

NAICS Code	Name
61	Educational Services
6113	Colleges, Universities, and Professional Schools

SOURCE REGIONS

Region	Asia

Subregion	Southern Asia
Countries	Iran

TARGET REGIONS

Region	Asia
Subregion	Western Asia
Countries	Jordan; Israel

THREAT DOMAINS

Cyber Espionage