

Application Security

9/1/2015
06:00 PM

Kelly Jackson Higgins
News

Connect
Directly

Cyberspies Impersonate Security Researcher

'Rocket Kitten' pro-Iranian regime hackers focusing more on targeting individuals for geopolitical espionage.

A cyber espionage group likely out of Iran turned the tables on a security researcher who may have gotten a little too close to its operation: the attackers posed as the researcher in a spear-phishing email.

The researcher, from ClearSky, has been tracking the hacking group, known as Rocket Kitten.

"[The researcher] had infiltrated … and was able to pose as a person of interest in this group, and they had engaged" with the researcher, says Jon Clay, senior global marketing manager for Trend Micro, which along with ClearSky today published new findings on Rocket Kitten. The spear-phishing email included a malicious link purportedly to a Trend Micro malware scanner.

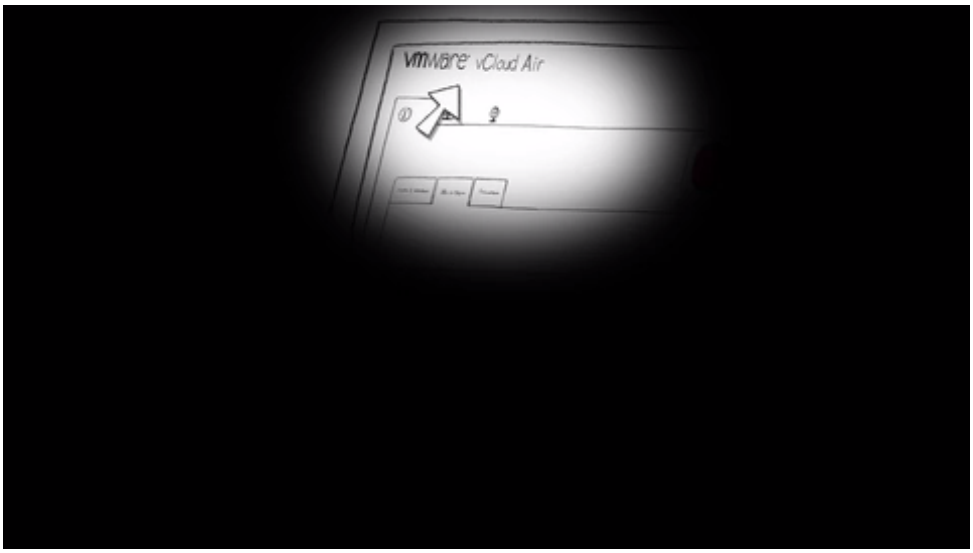


Image Source: Trend Micro

The attackers first attempted to contact the ClearSky researcher via a phony Facebook

profile, a ploy that ultimately failed. In late June, he learned that the attackers had sent a spear phishing email to one of their previous victims, Dr. Thamar E. Gindin, a lecturer on linguistics and pre-Islamic Iranian culture -- using his name as the purported sender. He had worked before Gindin while investigating Rocket Kitten's hacking activities, so the attackers either somehow had obtained previous email correspondence between the two, or they knew of the researcher's investigation into their operations.

"I can't tell what the hackers' motivation was to go after this individual [the ClearSky researcher]; it did give us some good information," Clay says. "We see this often with underground [cybercrime] investigations: a researcher infiltrates a forum and starts to be able to speak with the threat actors, acting like a member of the group."

This latest targeted attack demonstrates how Rocket Kitten's M.O. is now more about targeting individuals rather than organizations for the intel it's after, according to Trend Micro's findings. That's a departure from its earlier days, where the cyber espionage group went after organizations mostly in policy research, diplomacy, international affairs, defense, security, journalism, and human rights groups in the Middle East. Their targets of late appear to be Iranian dissidents and Israelis, more clues that Rocket Kitten is an Iranian attack group whose purpose is intelligence about the individual's activities. It's classic espionage with a geopolitical twist, researchers say.

"The interesting thing we found is that they shifted from going after organizations, to going after individuals associated with those organizations. They can then utilize this personalized data to get into the corporate data; they use that to leverage lateral movement inside the organization," Clay says. The goal is to steal the targeted individual's credentials, for example, to obtain a foothold in the targeted organization and move about "legitimately."

ClearSky has counted some 550 targets, mostly in the Middle East. "They are scientists, journalists, researchers, and sometimes expatriated Iranians living in Western countries. These facts suggest that Rocket Kitten may be engaging some sort of foreign political espionage campaign and may want to find regime-opponents active in driving policy in different ways," the Trend Micro and ClearSky report said. "These people are professionally affiliated with the foreign policy and defense sectors and there is an interest in finding out who they are talking to and what kinds of action they support."

Rocket Kitten isn't considered highly sophisticated; it uses simple hacking tools they may have written as well as pilfered publicly available ones. Researchers from CrowdStrike and Cymmetria, along with the Israeli CERT, late last year discovered that the cyber espionage group had used Core Security's penetration testing tool in their attacks.

While the Kitten group is doggedly persistent--they sometimes go after the same individual on a daily basis with different lures--they are known to make typos and grammatical errors that make them easy to spot, a characteristic often associated with cybercriminals. "However, the attackers do make up for these disadvantages with persistence. Based on our research and profiling, we believe the members of the Rocket Kitten Group could be former cybercriminals who ventured into a new field for some unclear reason and so use some of the methods they used to. Many of their techniques are typically observed in criminal endeavors," the report said.

Trend Micro's Clay says while identifying who's behind hacker groups is "tough," Rocket Kitten's targets appear to suggest it's a pro-Iranian government entity. The big challenge has been measuring the group's hacking success: "In a lot of cases, we're just seeing the initial attempts," Clay says. "We don't know what they are exfiltrating."

Kelly Jackson Higgins is Executive Editor at DarkReading.com. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise ... *View Full Bio*

Comments

BertrandW414,
User Rank: Strategist
9/2/2015 | 3:50:16 PM

Login

50%50%

That Cute Name

The name is "Rocket Kitten"? That's hilarious and adorable. Maybe that name sounds more menacing in Farsi. :-)

Reply | Post Message | Messages List | Start a Board

Newest First | Oldest First | Threaded View

Related Content

Sponsored by

RESOURCES BLOG TWITTER VIDEO

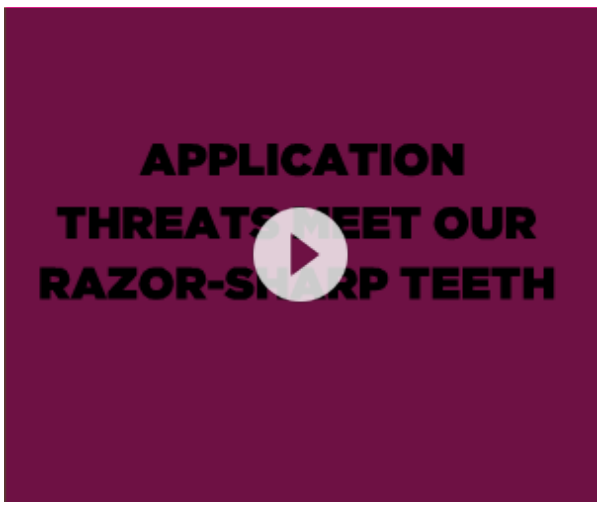
The New CISO's Tool Kit
Over the past few years, the view of the CISO as a high-level tactical asset has begun to change.

Secure Agile Development (Securosis)
This white paper is for security professionals who want to understand how to embed security into the Agile

G2000 Firm Secures Critical Financial Applications and Generates 192% ROI (Forrester)
Learn how a global firm secured 400 critical applications and

Hacking Exposed 7 - Chapter 10: Web and Database Hacking (McGraw-Hill)
Read this classic reference text to get into the cyberattacker's mind and understand the latest attack vectors

The Internet of Things: Security Research Study
As the Internet of Things (IoT) continues to gain traction and more connected devices come to market, security becomes a major concern.



Subscribe to Newsletters

Live Events Webinars

Latest Comment: great post good

Cartoon Archive

Current Issue

Dark Reading Tech Digest, June 2015

Download This Issue! Subscribe Now!

Back Issues | Must Reads

Flash Poll

What's missing from your incident response plan? (Pick all that apply.)

- [ ] Access to activity logs
- [ ] An up-to-date network diagram
- [ ] Blueprint for public disclosure
- [ ] Hostname-IP address maps
- [ ] IR fire drills before the event

- [ ] Plan for finding malicious files after the breach
- [ ] We don't have an incident response plan
- [ ] Other (Please explain in the comments)

Submit

All Polls

Reports Infographics

DevOps' Impact on Application Security

Managing the interdependency between software and infrastructure is a thorny challenge. Often, it's a "developers are from Mars, systems engineers are from Venus" situation.

Download Now!

More Reports

Slideshows

Sights & Sounds Of Black Hat USA And DEF CON

0 comments | Read | Post a Comment

Ouch! Feeling The Pain Of Cybersecurity In Healthcare 11

View From The Top: Government's Role In Cybersecurity 1

More Slideshows

Twitter Feed

Unisys Corporation @unisyscorp 6h
A tale of 2 outcomes: why #IoT #security remains a work in progress ubm.io/1KIXVky @DarkReading @kjhiggins pic.twitter.com/x2Qv2Hcp40
Retweeted by SecurityBot

Expand

Aaron Walker @4161726f6e 1m
New Shifu Banking Trojan An 'Uber Patchwork' Of Malware Tools darkreading.com/vulnerabilitie… via @DarkReading
Show Summary

Bug Report

Enterprise Vulnerabilities
From DHS/US-CERT's National Vulnerability Database

CVE-2015-3308

Published: 2015-09-02

Double free vulnerability in lib/x509/x509_ext.c in GnuTLS before 3.3.14 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted CRL distribution point.

CVE-2015-4330

Published: 2015-09-02

A local file script in Cisco TelePresence Video Communication Server (VCS) Expressway X8.5.2 allows local users to gain privileges for OS command execution via invalid parameters, aka Bug ID CSCuv10556.

CVE-2015-6274

Published: 2015-09-02

The IPv4 implementation on Cisco ASR 1000 devices with software 15.5(3)S allows remote attackers to cause a denial of service (ESP QFP CPU consumption) by triggering packet fragmentation and reassembly, aka Bug ID CSCuv71273.

CVE-2015-6277

Published: 2015-09-02

The ARP implementation in Cisco NX-OS on Nexus 1000V devices for VMware vSphere 5.2(1)SV3(1.4), Nexus 3000 devices 7.3(0)ZD(0.47), Nexus 4000 devices 4.1(2)E1, Nexus 9000 devices 7.3(0)ZD(0.61), and MDS 9000 devices 7.0(0)HSK(0.353) and SAN-OS NX-OS on MDS 9000 devices 7.0(0)HSK(0.353) allows remote...

CVE-2015-6587

Published: 2015-09-02

The vlserver in OpenAFS before 1.6.13 allows remote authenticated users to cause a denial of service (out-of-bounds read and crash) via a crafted regular expression in a VL_ListAttributesN2 RPC.

Dark Reading Radio

Archived Dark Reading Radio

Dark Reading at Black Hat: Highlights and Lessons

Another Black Hat is in the books and Dark Reading was there. Join the editors as they share their top stories, biggest lessons, and best conversations from the premier security conference.

FULL SCHEDULE | ARCHIVED SHOWS

Dark Reading
Enterprise Connect
GTEC
Gamasutra
Interop
Tower & Small Cell Summit

COMMUNITIES SERVED

Enterprise IT
Enterprise Communications
Game Development
Information Security
IT Services & Support

WORKING WITH US

Advertising Contacts
Event Calendar
Tech Marketing
Solutions
Contact Us
Licensing