SUPPORT CENTER (HTTPS://SUPPORTCENTER.CHECKPOINT.COM/SUPPORTCENTER/PORTAL?EVENTSUBMIT_DOHOME)

USER CENTER / PARTNERMAP (HTTPS://USERCENTER.CHECKPOINT.COM/USERCENTER/INDEX.JSP)

THREAT PREVENTION RESOURCES (HTTP://WWW.CHECKPOINT.COM/THREAT-PREVENTION-RESOURCES/INDEX.HTML)

(https://usercenter.checkpoint.com/)

Check Point SOFTWARE TECHNOLOGIES LTD. (http://www.checkpoint.com)

PRODUCTS / SOLUTIONS (HTTP://WWW.CHECKPOINT.COM/PRODUCTS-SOLUTIONS/)

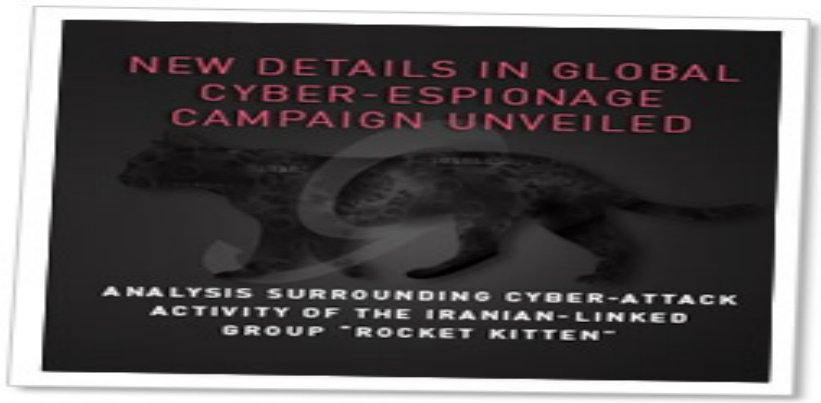
SUPPORT / SERVICES (HTTP://WWW.CHECKPOINT.COM/SUPPORT-SERVICES/)

PARTNERS (HTTP://WWW.CHECKPOINT.COM/PARTNERS/)

COMPANY (HTTP://WWW.CHECKPOINT.COM/ABOUT-US/)

Rocket Kitten: A Campaign With 9 Lives (http://blog.checkpoint.com/2015/11/09/rocket-kitten-a-campaign-with-9-lives/)

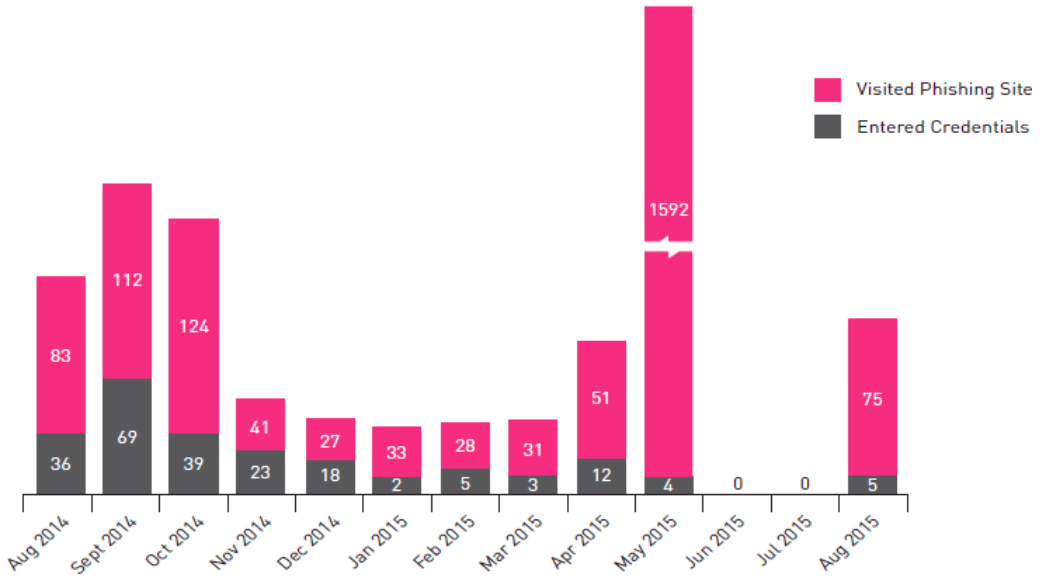
by Check Point Research Team posted 2015/11/09



(http://blog.checkpoint.com/2015/11/09/rocket-kitten-a-campaign-with-9-lives/)

The customized malware and creative phishing techniques of cyber-espionage groups prove that there is a recurring industry problem. Cyber criminals can evade detection by making minimal changes to most current protection solutions. Since early 2014, the attacker group dubbed 'Rocket Kitten' has been actively targeting organizations through malware infections and spear phishing campaigns. After an attack incident against a customer, Check Point researchers joined the investigations and released a report (http://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf) detailing the operations of the cyber-espionage campaign.

The Rocket Kitten group has been studied and analyzed on multiple occasions by different vendors, and these attacks have been linked to a global cyber-espionage campaign. They are known for extensively using various phishing schemes, along with custom-written malware, to execute their attacks. It has been reported that the group persistently e-mailed, called and responded with fake identities tailored for each victim – this clearly shows the creative mindset of the attackers as they read public reports about their targets and used it to adapt their tactics.



(http://blog.checkpoint.com/wp-content/uploads/2015/11/phishing-chart.png)

Phishing Logs and Successes Over Time

While the campaign has previously been made public by other researchers, the attacks did not stop. Instead, minimal changes were made to the groups' tools and phishing domains so that the attackers could continue targeting victims without interruption. In fact, the group remains active with reported attacks as recent as October 2015.

The targets of many successful attacks were individuals and organizations in the Middle East (including targets inside Iran itself), as well as across Europe and in the United States. In their investigation, Check Point researchers were able to access the victim database after the attackers failed to protect their phishing server. The target list contained 1600 targets, which included a very large campaign against scholars, scientists, CEOs, ministry officials, education institutes, media and journalists, and notable human rights activists.

This report (http://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf) describes the inner workings of Rocket Kitten, including an analysis of the target verticals, a chart of the attack timeline, and the true identity of the malware authors behind the campaign.

Download the full report 'Rocket Kitten: A Campaign with 9 Lives' here (http://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf).

Posted Under: Threat Research (http://blog.checkpoint.com/category/threat_research/)
Tags: cybercrime (http://blog.checkpoint.com/tag/cybercrime/), malware (http://blog.checkpoint.com/tag/malware/), phishing (http://blog.checkpoint.com/tag/phishing/), phishing attacks (http://blog.checkpoint.com/tag/phishing-attacks/), Threat Research (http://blog.checkpoint.com/tag/threat-research/)
Link to this post: http://blog.checkpoint.com/2015/11/09/rocket-kitten-a-campaign-with-9-lives/ ()

(http://blog.checkpoint.com/2015/11/06/why-its-a-smart-idea-to-use-threat-intelligence/)
Previous Post
Why it's a Smart Idea to Use Threat... (http://blog.checkpoint.com/2015/11/06/why-its-a-smart-idea-to-use-threat-intelligence/)

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Please complete the equation to verify your submission. *

+ six = 11

Start typing...

You may use these HTML (HyperText Markup Language) tags and attributes:

<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <s> <strike>

Post Comment

Post Archives

- November 2015 (http://blog.checkpoint.com/2015/11/)
- October 2015 (http://blog.checkpoint.com/2015/10/)
- September 2015 (http://blog.checkpoint.com/2015/09/)
- August 2015 (http://blog.checkpoint.com/2015/08/)
- July 2015 (http://blog.checkpoint.com/2015/07/)
- June 2015 (http://blog.checkpoint.com/2015/06/)
- May 2015 (http://blog.checkpoint.com/2015/05/)
- April 2015 (http://blog.checkpoint.com/2015/04/)
- March 2015 (http://blog.checkpoint.com/2015/03/)
- February 2015 (http://blog.checkpoint.com/2015/02/)
- January 2015 (http://blog.checkpoint.com/2015/01/)
- December 2014 (http://blog.checkpoint.com/2014/12/)
- November 2014 (http://blog.checkpoint.com/2014/11/)
- October 2014 (http://blog.checkpoint.com/2014/10/)
- September 2014 (http://blog.checkpoint.com/2014/09/)
- August 2014 (http://blog.checkpoint.com/2014/08/)
- July 2014 (http://blog.checkpoint.com/2014/07/)
- June 2014 (http://blog.checkpoint.com/2014/06/)
- May 2014 (http://blog.checkpoint.com/2014/05/)
- April 2014 (http://blog.checkpoint.com/2014/04/)
- March 2014 (http://blog.checkpoint.com/2014/03/)
- February 2014 (http://blog.checkpoint.com/2014/02/)
- January 2014 (http://blog.checkpoint.com/2014/01/)
- December 2013 (http://blog.checkpoint.com/2013/12/)
- November 2013 (http://blog.checkpoint.com/2013/11/)
- October 2013 (http://blog.checkpoint.com/2013/10/)
- August 2013 (http://blog.checkpoint.com/2013/08/)
- July 2013 (http://blog.checkpoint.com/2013/07/)
- January 2013 (http://blog.checkpoint.com/2013/01/)

- December 2012 (http://blog.checkpoint.com/2012/12/)
- November 2012 (http://blog.checkpoint.com/2012/11/)

Search

RSS (http://blog.checkpoint.com/feed/)

Products

Next Generation Threat Prevention (http://www.checkpoint.com/products-solutions/threat-prevention/)
Mobile Security (http://www.checkpoint.com/products-solutions/mobile-security/)
Next Generation Firewalls (http://www.checkpoint.com/products-solutions/next-generation-firewalls/)
Security Management (http://www.checkpoint.com/products-solutions/security-management/)
Products A-Z (http://www.checkpoint.com/products-solutions/all-products/)
30-Day Free Trial (http://www.checkpoint.com/try-our-products/)
Find a Partner (http://partners.us.checkpoint.com/partnerlocator/)
Contact Sales (http://www.checkpoint.com/about-us/contact-us/)

Threat Prevention Resources

IPS Advisories & Protections (http://www.checkpoint.com/advisories/)
Under Attack? (http://www.checkpoint.com/support-services/threatcloud-incident-response/)
World Cyber Threat Map (https://www.checkpoint.com/ThreatPortal/livemap.html)

Support and Services

Support Center (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doHome)
Support Plans (http://www.checkpoint.com/support-services/support-plans/)
Training and Certification (http://www.checkpoint.com/support-services/training-certification/)
Forums (https://forums.checkpoint.com/)
Design, Deploy, Operate and Optimize (http://www.checkpoint.com/support-services/design-deploy-operate-optimize/)
Lifecycle Management Services (http://www.checkpoint.com/support-services/lifecycle-management/)
Contact Support (http://www.checkpoint.com/support-services/contact-support/)

Partners

Become a Partner (http://www.checkpoint.com/partners/channel/)
Find a Partner (http://partners.us.checkpoint.com/partnerlocator/)
User Center Sign In (https://usercenter.checkpoint.com/usercenter/index.jsp)

Solutions and Architecture

Retail / Point of Sale (POS) (http://www.checkpoint.com/products-solutions/retail-point-of-sale-pos/)
Financial Services (http://www.checkpoint.com/products-solutions/financial-services-atm/)
Critical Infrastructure (http://www.checkpoint.com/products-solutions/critical-infrastructure/)
Private & Public Cloud (http://www.checkpoint.com/products-solutions/private-public-cloud/)
Healthcare (http://www.checkpoint.com/products-solutions/healthcare/)
Service Provider / Telco (http://www.checkpoint.com/products-solutions/service-provider-telco/)
Software Defined Network (SDN) (http://www.checkpoint.com/products-solutions/software-defined-network/)
Governance, Risk & Compliance (http://www.checkpoint.com/products-solutions/governance-risk-compliance/)
Software Defined Protection (SDP) (http://www.checkpoint.com/products-solutions/software-defined-protection-sdp/)

Company

Facts at a Glance (http://www.checkpoint.com/about-us/facts-a-glance/)
Our History (http://www.checkpoint.com/about-us/our-history/)
News (http://www.checkpoint.com/about-us/news-coverage/)
Blog (http://blog.checkpoint.com)
Events (http://store.checkpoint.com/events/eventsindex.htm)
Contact Us (http://www.checkpoint.com/about-us/contact-us/)
Search Jobs (http://careers.checkpoint.com/)

Follow Us

(https://twitter.com/checkpointsw) (https://plus.google.com/+checkpoint/posts)
(https://www.facebook.com/checkpointsoftware
(https://www.youtube.com/channel/UCXnlgfiXZ0 8ZKA?sub_confirmation=1) (http://www.checkpoint.com/rss/)

©2015 Check Point Software Technologies Ltd. All rights reserved. Check Point Software Technologies, Inc. is a wholly owned subsidiary of Check Point Software Technologies Ltd.

Copyright (http://www.checkpoint.com/copyright/) | Privacy Policy
(http://www.checkpoint.com/privacy/) | Site Map (http://www.checkpoint.com/site-map/)