Rocket Kitten Showing Its Claws: Operation Woolen-GoldFish and the GHOLE campaign

trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing

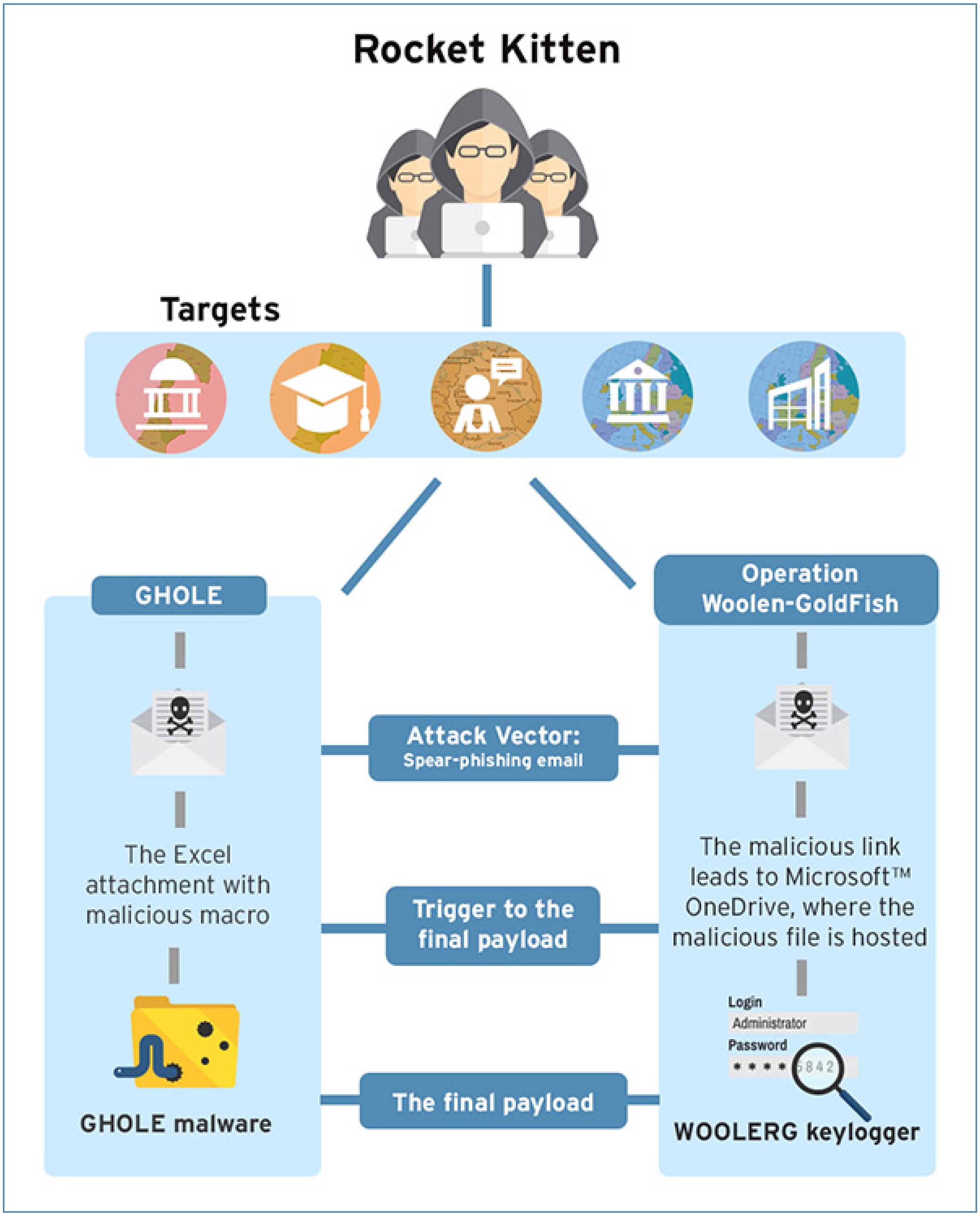
View research paper: Operation Woolen Goldfish: When Kittens Go Phishing

Rocket Kitten refers to a cyber threat group that has been hitting different public and private Israeli/European organizations. It has launched two campaigns so far: a malware campaign that exclusively makes use of GHOLE malware, as well as a targeted attack dubbed as “Operation Woolen-GoldFish” that's possibly state-sponsored.

GHOLE is a malware family that was discussed in the 31st Chaos Communication Congress of the Chaos Computer Club (31C3), during a lecture that tackled its ongoing involvement in targeted attacks. Based on the compilation date of its oldest samples, the malware is believed to have been active since 2011, and has been used by Rocket Kitten in their targeted attacks.

Operation Woolen-GoldFish, on the other hand, is a cyber attack campaign that we suspect to be state-sponsored, or at the very least politically-motivated. It has been attacking the following targets:

- Civilian organizations in Israel
- Academic organizations in Israel
- German speaking government organizations
- European government organizations
- European private companies


Rocket Kitten
Targets
GHOLE
Operation Woolen-GoldFish
Attack Vector:
Spear-phishing email
The Excel attachment with malicious macro
Trigger to the final payload
The malicious link leads to Microsoft™ OneDrive, where the malicious file is hosted
Login
Administrator
Password
****5842
GHOLE malware
The final payload
WOOLERG keylogger

Background, Analysis, Findings

GHOLE Malware Campaign:

- In February 2015, we received an alert that involved an infected Excel file that, upon analysis, proved to be part of the GHOLE malware campaign, one of Rocket Kitten's campaigns.

- The GHOLE malware campaign involves victims being sent spear-phishing emails with malicious attachments. The attachment is usually an Excel file that contains a malicious macro.
- When clicked, the Excel file drops a .DLL file that will then be executed by the malicious macro embedded in the Excel file.
- The Excel file is tailored to trick the user into running the macro. If the user does not enable the macro content, the .DLL file will not be executed.
- GHOLE is a malware family derived from a modified Core Impact product. Core Impact is a penetration-testing product made by Core Security, a legitimate company.
- Further analysis revealed that the GHOLE variants involved in the operation connect to C&C servers hosted mainly in Germany. The servers are registered under one customer by the name of Mehdi Mavadi. We are hesitant in attributing the attack to such an identity as the name itself is quite common, and that the customer's servers may simply be compromised and being used as a proxy rather than actually providing infrastructure for the Rocket Kitten group.

Operation Woolen-GoldFish:

- Similar to the GHOLE malware campaign, Operation Woolen Goldfish involves spear-phishing emailsembedded with a malicious link that leads to a OneDrive link. The link goes directly to a malicious file download.
- The malware payload was initially found to be a variant of GHOLE, but further samples led to te discovery of a new payload: a variant of a keylogger known as the CWoolger keylogger. It is detected as TSPY_WOOLERG.A.

Possible Attribution

Analyzing the malicious documents in the spear phishing emails of their Microsoft Office metadata, we narrowed down the suspects to one "Wool3n.H4t", whose name appears in most of the document samples found as the last known modifier. His other accomplices include entities who go by the names "aikido1" and "Hoffman".

We looked deeper into the identity of Wool3n.H4t and discovered the following:

- He may have been running an underground hacking blog under the same nickname, with the only two entries signed by "Masoud_pk"
- "Masoud_pk" may possibly be the true identity of Wool3n.H4t. "Masoud" belongs in the top 500 commonly used first names in Iran.
- A debug string found in the CWoolger keylogger code shows that the compiler is identified as Wool3n.H4T.

Conclusion

This report explores Rocket Kitten by analyzing the tools used to leverage its malicious activities. From our findings we can definitely say that threat actor team is alive and active, and while the tracks they left behind—as well as their use of macros—might make them seem a bit inexperienced, they are slowly improving and gaining traction.

We are also able to confirm that Wool3n.H4T is not only responsible for most of the infecting Office documents used, but also capable of developing malware.

With all the evidence, Rocket Kitten's attacks can be construed as politically-motivated, as the targeted entities do share a particular interest in the Islamic Republic of Iran. While motives behind targeted attack campaigns differ, the end results are one and the same: shift in power control either in the economically or politically.

Read the research paper Operation Woolen-GoldFish: When Kittens Go Phishing for a full, detailed look into the activities and methods of Rocket Kitten.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below.   2. Press Ctrl+A to select all.   3. Press Ctrl+C to copy.   4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cyber Attacks, Research, Phishing, Cybercrime, Targeted Attacks