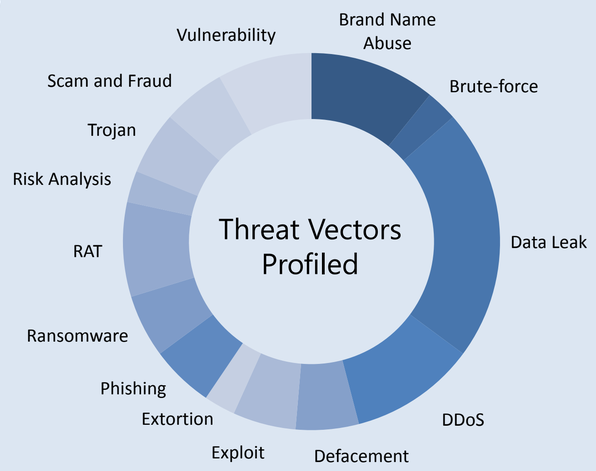
THE MONTHLY

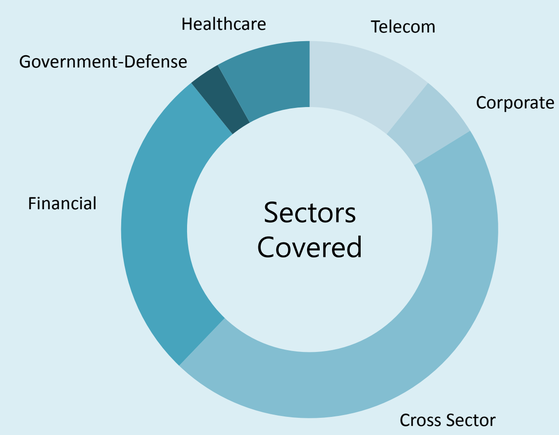
CYBER THREAT INSIDER

JUNE 21, 2017
EDITION 9

TAILORED THREAT INTELLIGENCE: MONTHLY OVERVIEW

SenseCy uses a unique methodology to source a multitude of web-platforms, including deep web forums, darknet marketplaces, closed social media groups, mobile apps and more, producing actionable intelligence alerts and expert reports for its customers. Here is a breakdown of the sectors covered and the threat vectors profiled in the past 30 days:





#OPICARUS CYBER CAMPAIGN – ROUND 5

Hacktivists recently launched the fifth phase of the #OpIcarus cyber campaign (also dubbed #OpSacred) against the financial sector around the world. This campaign was first launched in February 2016, and as in previous phases, the official target list contains mainly websites of central banks around the world. In addition, the initiators share links to download known DDoS tools, such as TorsHammer or XerXes.

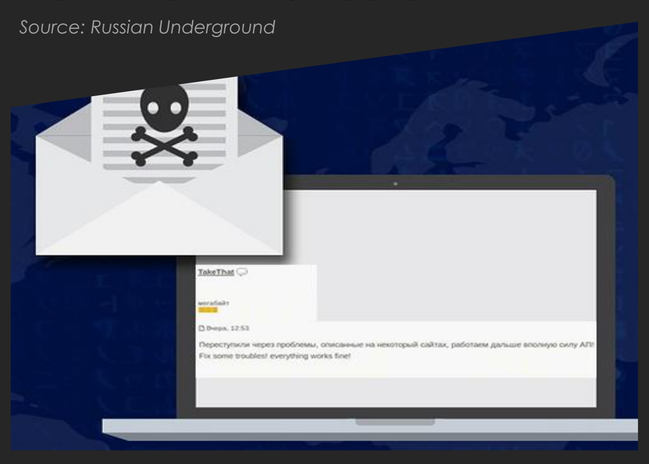
The official event page states that this phase will take place between June 7 and 21, 2017 (to date, 71 Facebook users approved their participation). However, participants have already claimed responsibility for allegedly shutting down several websites of central banks around the world.

The second phase of #OpIcarus campaign, which took place during May 2016, was the most popular among hacktivists that carried out DDoS attacks (some even successful, according to news reports) targeting websites of financial institutions around the world. Additional phases launched afterward did not manage to gain the same level of popularity or achievements.

Share this blog post

RIG EXPLOIT KIT RE-EMERGES AFTER MASSIVE OPERATION TO TAKE DOWN ITS INFRASTRUCTURE

Source: Russian Underground



The gang of Russian cybercriminals behind the operation of the RIG EK has posted on a Deep Web forum that they are fully recovered from "problems" that arose following coordinated effort to disrupt their activities in early June. The message was posted several days after the press releases about the operation.
In reply to this post, RIG users indicated that the success rate of the EK had decreased significantly (probably because the Silverlight exploit no longer works). But it is now functioning again.
SenseCy analysts assess that with no good alternatives being traded publicly, RIG will continue to dominate the EK market in the near future.

HACKTIVISTS PROTEST AGAINST THE YULIN DOG MEAT FESTIVAL, SHUTTING DOWN CHINESE .GOV WEBSITES

Source: Social Media

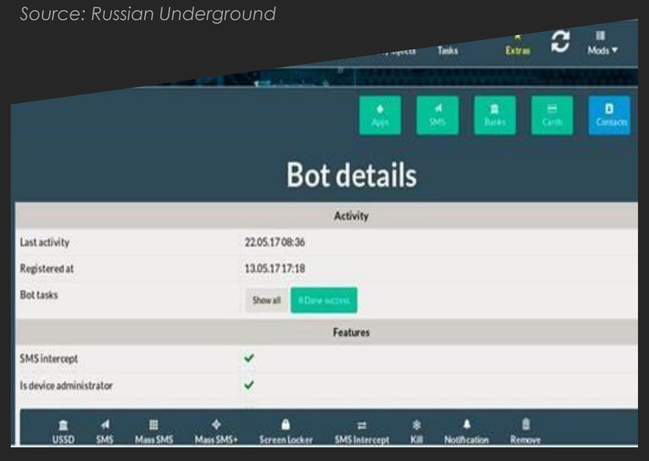
The Yulin Dog Meat Festival, scheduled to take place between June 21 and 30, 2017, has attracted the attention of hacktivist threat actors, who already claimed responsibility for shutting down several Chinese government websites during May 2017. It is possible that there will be additional cyber-attacks against Chinese websites in the following two weeks.

TERM OF THE MONTH: OVERLAY ATTACK

"The main technique employed nowadays in Android Trojans, also called by cybercriminals "mobile injections", though it slightly differs from the classic web-injections for Desktop Banking Trojans."

SHARP RISE IN ANDROID TROJANS ADVERTISED ON CYBERCRIME FORUMS

Source: Russian Underground



SenseCy analysts have identified a prominent rise in the number of Android Trojans traded on Deep Web forums dedicated to cybercrime.
With more than 10 different Trojans, currently selling for between $500 and $2,000 per month, it appears that cyber-crooks have identified a gap in the security level of mobile devices, which they are trying to exploit for financial theft. All of the Trojans implement the overlay app attack to mimic official apps of financial services.

NEW MARKET TRENDS SURFACE IN THE DARKNET

Source: Darknet

In recent weeks, we have observed a new trend developing on the Darknet, when new hidden services solicit users to invest funds in Darknet markets.
One of the services even functions as a loan service for Darknet market vendors, promising a minimum monthly profit of 40% of the loan.

INVITE YOUR CONTACTS TO SUBSCRIBE