Security

20KB trojan turns on bank customers in Singapore, Indonesia

Fifth Tinba iteration 'Tinbapore' found and flagged

19 Jan 2016 at 06:33, Darren Pauli

The infamous Tinba trojan has been updated and is now targeting people using online banking in the Asia Pacific region.

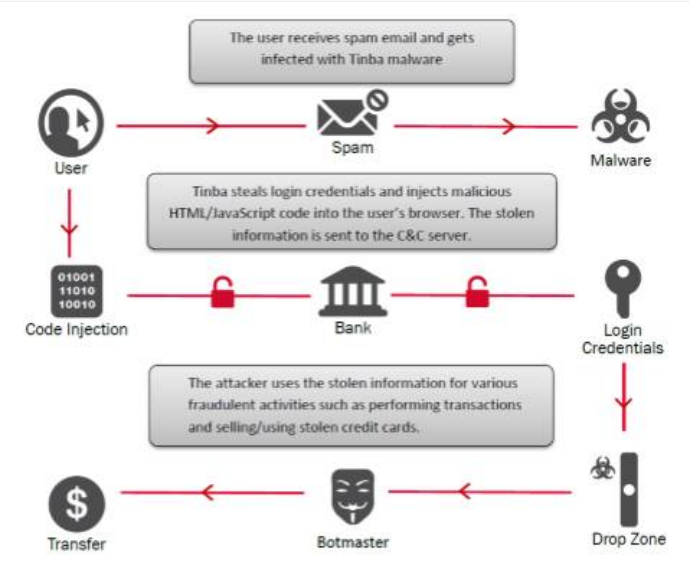
Malware bods from security company F5 refer to the fifth iteration of the Windows software nasty as Tinbapore since it began moving 70 percent of its infection base to the region.

About 30 percent of infections are located Singapore and 20 percent in Indonesia. Only five percent are in Australia.

"Newer and improved versions of the malware employ a domain generation algorithm, which makes the malware much more persistent and gives it the ability to come back to life even after a command and control server is taken down," the researchers say (PDF).

"This new variant of Tinba, Tinbapore, now creates its own instance of *explorer.exe* that runs in the background.

"It differs from most previous versions in that it actively targets financial entities in the Asian Pacific which was previously uncharted territory for Tinba."



Tinba, also known as Tinybanker, Zusy, and HµNT€R$, was a bite size 20KB online-bank-account-raiding trojan first seen in May 2012.

Source code leaked in July 2011 when net scum grabbed and customised their own sophisticated builds to target banks around the world. ®

Sponsored: Why every enterprise needs an Internet Performance Management (IPM) Strategy

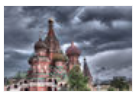
Tips and corrections

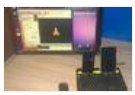
9 Comments

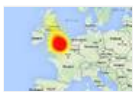
More like this

Malware Security

Most read


'I bet Russian hackers weren't expecting their target to suck so epically hard as this'


Intel shows budget Android phone powering big-screen Linux

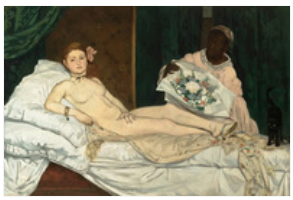

Between you, EE and the lamppost ... this UK cell network is knackered


FBI v Apple spat latest: Bill Gates is really upset that you all thought he was on the Feds' side


Hackers aren't so interested in your credit card data these days. That's *bad news*

Spotlight

More from The Register



Nude tribute to Manet's *Olympia* ends in cuffing

Disrobed performance artist rumpus at Paris's Musée d'Orsay

48 Comments

GCHQ Christmas Card asks YOU the questions

Festive puzzler promises cryptographic and charity payload

59 Comments

NICE catch, Amazon: Bezos buys HPC toolkit from Italy

Is Uncle Jeff's cut-price bit-barn rental company contemplating HPCaaS?

3 Comments

GCHQ intel used to develop Stuxnet, claims new documentary

US peppered Iran with thousands of cyberwar weapons

20 Comments

GCHQ goes all Cool Dad and tags the streets of Shoreditch with job ads

IBM tried something similar in 2001, and copped a fine

51 Comments

GCHQ creates Github repo, offers graph database code

Running an intelligence agency's super-database – what could go wrong with that?

21 Comments

Whitepapers

8 data threat trends you must defend against immediately

Forcepoint Security Labs experts tell you what you need to do to prepare for what lies ahead.

What's Wrong with Disaster Recovery?

One serious outage or natural disaster can be enough to threaten the continued existence of the organisation. So what's wrong with DR?

Defend against the undetected

The old ways of defending your network against attackers and cybercriminals have limited effectiveness in today's world.

The 2016 Cyber Risk Executive Summary

Hacker attacks are evolving to target applications and to focus on financial gain. This report brings you the key findings and conclusions of this year-long research effort.

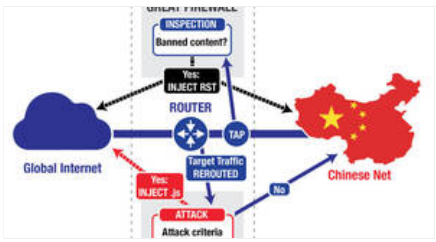
Row over GCHQ-built voice algo MIKEY SAKKE rumbles on

Techie on the ground disputes BlackEnergy Ukraine power outage story

Asda slammed for letting vulns fester on its cyber shelves

Australia and America working on global no-state-hacking pact

PDF redaction is hard, NSW Medical Council finds out - the hard way



What if China went all GitHub on your website? Grab this coding tool

Invite-only bug bounty criticised for turning up the heat on Tor

Law enforcement versus Silicon Valley's idle problem children

Sponsored links

Sydney.