SANS ISC: Sasfis Propagation - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

isc.sans.edu/forums/diary/Sasfis+Propagation/8860/

Sasfis Propagation

Naming and tracking different malware families still leaves much to be desired, so for lack of a better alternative, I'm using the term Sasfis. It's function appears to be a general bot-net and is mostly leveraged to install other malware such as key-logging/banking-trojans such as Zeus or scareware like the many variants of Fake Anti-virus that is currently in the wild.

I've been seeing this payload quite often this week. The most common way I see it is in fake shipping invoices. Today I received a well-targeted email using obviously-compromised user-contact data. It claimed to be from the state business tax department, and encouraged the recipient to install the (fake) secure-gateway software so that they could continue to pay their sales taxes online.

I'm being intentionally vague about the state since I'm haven't been able to contact them (abuse@$STATE$.gov bounces, for shame) but needless to say, if your state is distributing security software to you, it shouldn't be hosted in Moldova.

The detection of the malware was low, only 3 out of 40 at virus total. The host of the command and control server is also well aware of certain public sandboxes' IP addresses; their reports of network behavior were obviously blocked, and I managed to get one of my test IP addresses similarly blocked while playing around with the code today. They're upping their game.
For those looking for this on their networks, look for HTTP-like activity out to v-medical.org and 89.187.53.203.

Kevin Liston

292 Posts
ISC Handler
May 27th 2010

Thread locked Subscribe

May 27th 2010
1 decade ago

The activity and netblock you mention makes me think that this is related to Bredolab.

http://blog.trendmicro.com/bredolab-revealed/

Check out the PDF near the bottom.

Anonymous

Quote

May 27th 2010
1 decade ago

Yeah, Bredolab, Sasfis, Agent, Outbreak... pick one. 🙂

Kevin Liston

292 Posts
ISC Handler

Quote	May 27th 2010 1 decade ago
Would you kindly link the virustotal or post the hash, size, filename, etc?	hacks4pancakes  48 Posts
Quote	May 28th 2010 1 decade ago
virustotal.com/analisis/…	Kevin Liston  292 Posts ISC Handler
Quote	May 30th 2010 1 decade ago