Snort rules for Iodine Covert DNS Tunnel Detection

Posted by merc in Intrusion Detection on Jul 26th, 2009 | 2 comments
I created two Snort IDS rules to detect covert Iodine tunnels.Â Frequently in corporate environment and WIFI hotspots, DNS is not blocked at the firewalls and is allowed to flow to the internet while other type of traffic is restricted. Iodine lets users take advantage of this fact and allow tunneling IPv4 trafficÂ over DNS queries.Â These Snort rules were tested with Iodine version 0.4.2, I'm very interested in getting feedback on how the rules are working (or not for you) or how I could make them better. You can find the Iodine Snort rules at this location:
http://www.securitywire.com/snort_rules/iodine.rules

2 Responses to " "Snort rules for Iodine Covert DNS Tunnel Detection"

1. *waydaws* says:
March 28, 2010 at 19:49

I guess this has been posted for awhile, but I should comment anyway.

The first thing I thought when I saw the rule was "what if they used tcp."

I know people think it's only used for zone transfers, but that not the case. With EDNS (extensions) now enabled pretty much everywhere, if an answer to a query is too large for a single udp packet, it can switch to tpc/53.

A couple of years ago, when I was still responsible for DNS, we got sporadic, but steady complaints about mail delivery failures. I eventually found that it happened when we were getting replies back from companies like hp.com that had numerous IPs under one MX host name (and vice versa).
Some investigation showed the network team had, among other things, enabled EDNS blocking on a PIX Firewall following Cisco "recommended secuirty best practices". From there it was

easy to fix, but it brought it home to me that simple fire wall rules like allow only udp/53 to a NS server can be a problem.

Likewise, in your case, you may be not watching everything. I admit that since I haven't used Iodine, maybe they don't have an option to use tcp, but someone might have thought about the capability and added it, should that be the case.

Reply

2.  *Dave* says:
July 6, 2010 at 20:34

Do you know how to block iodine with pfense and snort? is there are special command ?

Reply

Leave a Reply

Your email address will not be published.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

Name *

Email *

Website

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Submit Comment

About Me

about us image

Michel Chamberland is a **Security Solutions Architect** in the United States with over 15 years of experience in the full software development life cycle (SDLC) with a focus on security. He achieved numerous certifications including GIAC, C|HFI, C|EH, CCNA, CCNA Security, CCSK, Security+, Network+, A+, Project+, MCTS, MCP and Various CIW.

Categories

- Cryptography
- Exploits
- Forensics
- Intrusion Detection
- Links
- Penetration Testing
- Protection
- Protocols
- Reverse Engineering
- Secure Development
- Security News
- SecurityWire
- Tools
- Vulnerability Research

Sponsor

IPv6 Status

Status: *IPv6 Enabled*
Last: *2013-03-11*

PGP Key | Sitemap