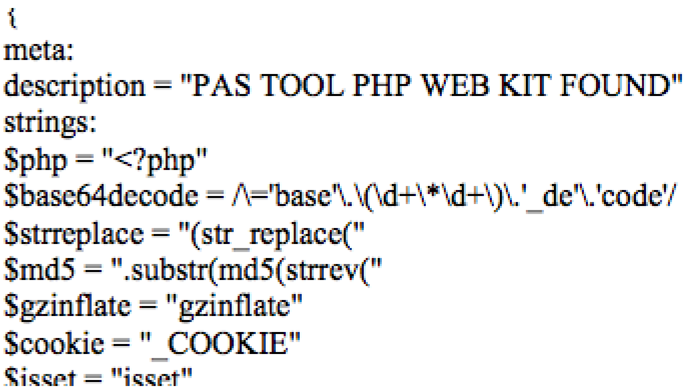
Some notes on IoCs

blog.erratasec.com/2016/12/some-notes-on-iocs.html

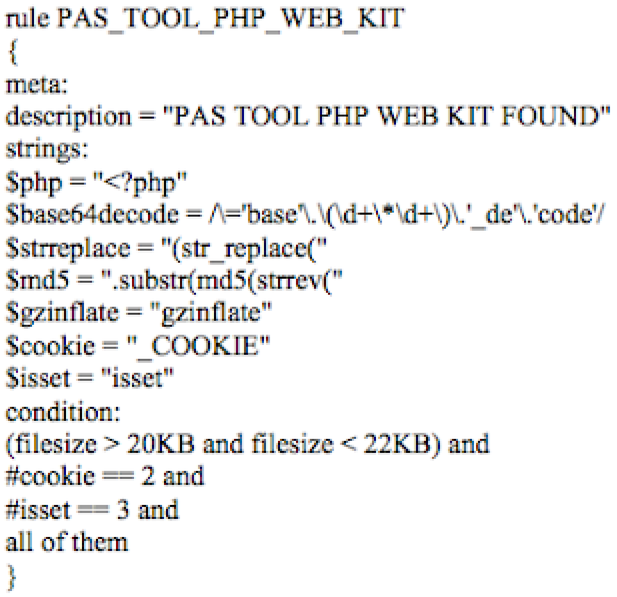


```
{
meta:
description = "PAS TOOL PHP WEB KIT FOUND"
strings:
$php = "<?php"
$base64decode = /\='base'\.\(\d+\*\d+\)\.'_de'\.'code'/
$strreplace = "(str_replace("
$md5 = ".substr(md5(strrev("
$gzinflate = "gzinflate"
$cookie = "_COOKIE"
$isset = "isset"
```

Obama "sanctioned" Russia today for those DNC/election hacks, kicking out 35 diplomats (**), closing diplomatic compounds (**), seizing assets of named individuals/groups (***). They also published "IoCs" of those attacks, fingerprints/signatures that point back to the attackers, like virus patterns, file hashes, and IP addresses.

These IoCs are of low quality. They are published as a political tool, to prove they have evidence pointing to Russia. They have limited utility to defenders, or those publicly analyzing attacks.

Consider the Yara rule included in US-CERT's "GRIZZLY STEPPE" announcement:



```
rule PAS_TOOL_PHP_WEB_KIT
{
meta:
description = "PAS TOOL PHP WEB KIT FOUND"
strings:
$php = "<?php"
$base64decode = /\='base'\.\(\d+\*\d+\)\.'_de'\.'code'/
$strreplace = "(str_replace("
$md5 = ".substr(md5(strrev("
$gzinflate = "gzinflate"
$cookie = "_COOKIE"
$isset = "isset"
condition:
(filesize > 20KB and filesize < 22KB) and
#cookie == 2 and
#isset == 3 and
all of them
}
```

What is this? What does this mean? What do I do with this information?

It's a YARA rule. YARA is a tool ostensibly for malware researchers, to quickly classify files. It's not really an anti-virus product designed to prevent or detect an intrusion/infection, but to analyze an intrusion/infection afterward -- such as attributing the attack. Signatures like this will identify a well-known file found on infected/hacked systems.

What this YARA rule detects is, as the name suggests, the "PAS TOOL WEB KIT", a *web shell* tool that's popular among Russia/Ukraine hackers. If you google "PAS TOOL PHP WEB KIT", the second result points to the tool in question. You can download a copy here [*], or you can view it on GitHub here [*].

Once a hacker gets comfortable with a tool, they tend to keep using it. That implies the YARA rule is useful at tracking the activity of that hacker, to see which other attacks they've been involved in, since it will find the same web shell on all the victims.

The problem is that this P.A.S. web shell is popular, used by hundreds if not thousands of hackers, mostly associated with Russia, but also throughout the rest of the world (judging by hacker forum posts). This makes using the YARA signature for attribution problematic: just because you found P.A.S. in two different places doesn't mean it's the same hacker.

A web shell, by the way, is one of the most common things hackers use once they've broken into a server. It allows further hacking and exfiltration traffic to appear as normal web requests. It typically consists of a script file (PHP, ASP, PERL, etc.) that forwards commands to the local system. There are hundreds of popular web shells in use.

We have little visibility into how the government used these IoCs. IP addresses and YARA rules like this are weak, insufficient for attribution by themselves. On the other hand, if they've got web server logs from multiple victims where commands from those IP addresses went to this specific web shell, then the attribution would be strong that all these attacks are by the same actor.

In other words, these rules can be a reflection of the fact the government has excellent information for attribution. Or, it could be a reflection that they've got only weak bits and pieces. It's impossible for us outsiders to tell. IoCs/signatures are fetishized in the cybersecurity community: they love the small rule, but they ignore the complexity and context around the rules, often misunderstanding what's going on. (I've written thousands of the things -- I'm constantly annoyed by the ignorance among those not understanding what they mean).

I see on twitter people praising the government for releasing these IoCs. What I'm trying to show here is that I'm not nearly as enthusiastic about their quality.

Note#1: BTW, the YARA rule has to trigger on the PHP statements, not on the imbedded

BASE64 encoded stuff. That's because it's encrypted with a password, so could be different for every hacker.

Note#2: Yes, the hackers who use this tool can evade detection by minor changes that avoid this YARA rule. But that's not a concern -- the point is to track the hacker using this tool across many victims, to attribute attacks. The point is not to act as an anti-virus/intrusion-detection system that triggers on "signatures".

Note#3: Publishing the YARA rule burns it. The hackers it detects will presumably move to different tools, like PASv4 instead of PASv3. Presumably, the FBI/NSA/etc. have a variety of YARA rules for various web shells used by know active hackers, to attribute attacks to various groups. They aren't publishing these because they want to avoid burning those rules.

Note#4: The PDF from the DHS has pretty diagrams about the attacks, but it doesn't appears this web shell was used in any of them. It's difficult to see where it fits in the overall picture.

(**) No, not really. Apparently, kicking out the diplomats was punishment for something else, not related to the DNC hacks. (***) It's not clear if these "sanctions" have any teeth.