Static Hostname "RULER" #47

New issue

Closed **passwordleak** opened this issue on Aug 3, 2017 · 3 comments

passwordleak commented on Aug 3, 2017 • edited

I was just checking the logs to look for defenses, and I realized that the hostname is always "RULER," even when I change the user agent, which is also "ruler."

From an attacker perspective, this obviously limits value as the defender can just look for hostname RULER events, so I grepped for "ruler" but could not find any relevant code, so I think it may be in a binary file or something. Of course skids will still use the default so defenses can still pick up on them.

I'm wondering if this "RULER" hostname can be changed.

1

staaldraad commented on Aug 4, 2017 Collaborator

Brilliant! I've been waiting for a year to have someone ask this question :)

The hostname and the user-agent were hard-coded to give blue-teams a starting point. Basically a skiddy "canary"

I've buried the hostname in the supporting NTLM library; https://github.com/staaldraad/go-ntlm - more specifically, in ntlmv1.go and ntlmv2.go.

```
am.Workstation, _ = CreateStringPayload("RULER")
```

Awesome that you've dug in and looked into this!

1

staaldraad closed this as completed on Aug 4, 2017

lnxg33k commented on Sep 20, 2017

Any plans to parameterize the workstation name along with the User-Agent (for all HTTP(s) requests) ?!

staaldraad commented on Sep 20, 2017 Collaborator

Nope sorry, not thinking of it at present :)
Happy to accept PRs though!

2

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants