WNAG

Meeting: 2017-05-17
Present: Jim Johnston (Chair), Anton Romantsov (Secretary), Lowell Williamson, Bernie Rutter, Allan Fleming, Nevil Bromley, Ray White, Manfred Griesbach, David Aldwinckle, Dave Hinton, Mark Gaulton, Mike Patterson, Julio Gonzalez

MalwareBytes for Business presentation (Doug Smith via RingCentral conference call).

Highlights (as submitted to the Agenda - thanks Manfred):

- Offers a new capability called Malware Hunting (proactive intrusion assessment)
- Complements reactive traditional A/V
- Supports PCs and Macs (soon Android)
- Is a remediation and anti-exploit tool
- Does not rely on signatures, white listing, sandboxing or VMs
- Protects against attacks and zero-hour malware
- Is fully AD integrated – meaning no/little user administration on server (all from Nexus)
- Leverages SCCM for agent deployment (also runs agentless)
- Have choice of cloud server or in-house
- Initial offer: $10.50/yr/client for a 3-yr contract
- Full delegation of control on central console
- IST will be evaluating an in-house server solution, starting with IST clients

Questions:

Mike: How licensing works? pricing?
Doug: We will work together to reduce costs and find a number that works for all.
Mike: We're only looking at staff for Malwarebytes, not undergrads.
Manfred: Any technical questions?
Mark: We will continue offline.
Jim: What's the plan?
Mark: PoC on 300 endpoints, deploy real-time scanning and manage agents from console. IST will have that deployed first, some seats will be available for all campus to try. The agent is very light on footprint, deployed via SCCM, updates come from the MB server.

New Business

Jim: RODC on the agenda, where we are right now?

Dave H: We installed RODC in Test.
Julio: Engineering proposed RODC to mitigate the problems they reported earlier (GPMC crashing and network disconnects). We will create a new site in AD and will install two RODCs that will serve Engineering users coming from the network subnets used by Engineering.
Jim: Issues reported by Engineering – are they still seeing network drives dropping?

Julio: We haven't been able to reproduce the problem ourselves. On a test machine, we run a script hitting network every 3 seconds, so far it never failed. We asked Engineering for assistance to reproduce; last communication about this was a week ago.
Jim: In the email that Engineering sent to WNAG, it was stated that the problem was reproducible.
Ray: It is reproducible.
Jim: Reproducible means we can define enough of the factors and conditions to trigger the bad behaviour on demand; otherwise it is just a recurring problem. You approach debugging these problems differently. Which is this?
Ray: You tell me.
Jim: I'm asking how this was approached and investigated, what are your findings today? My biggest worry is that politics is interfering with collaboration.

Jim: We can volunteer and help debugging this problem if Engineering interested.
Ray: Typically, we deal with GPOs after the end of the term. We try not to do anything with workstations while users are using them. We did it two weeks ago.
Jim: Understood and agreed. But, now is when you have time to debug. If it doesn't happen when you're testing - that is not reproducible. We can generate domain load to see how endpoints are affected. You might need to cooperate by doing what you do not normally do during the term (update some test PCs) to allow investigation to continue.
Jim: We all want a stable domain, we all have same goal here; what can we do as a group to help?
Dave A: We were working with Ray and it seems getting no issue on netapp level, we will continue with this.
Jim: When Engineering stood up the RODC – did you actually see the problem to go away?
Ray: It was up only for a day.
Jim: Okay. So, you were not able to confirm the outcome in such a short interval?
Ray: Exactly.
Jim: The original statement posted to WNAG said that the problem was reproducible, but in reality it sounds like you cannot reproduce it – it is recurring, not reproducible. Or, do you know how can we reproduce it?
Ray: I don't know how to answer that.

Jim: We're getting to a certain point when things starting to get out of our hands.
Ray: Debugged was done on the same site we all have access to. We had to try something to move on and we tried RODC.
Jim: Is there something anyone of us can help to debug this?
Ray: We have done a number of different things and the amount of times it is failing has gone down to zero on our test computer. RODC doesn't cost us much in terms of risk and is a simple thing to do.
Jim: By putting in RODC without proper sites, we can't limit authentication to only select group of users. How could the originally installed RODC prevent authentication by other users?
Julio: The new setup will have RODC placed in a new site and it will be caching credentials for users only in selected Engineering groups.
Jim: Note that even if RODC solves the problem for your users while inside your site, you could still see delays when your people are outside of your site and will be authenticating on other DCs. E.g. your profs on podiums and students in non-Eng labs.

Jim: Are there any other concerns operating RODC?
Dave H: It will not be behind IST firewall, it will be behind Engineering firewall outside of IST machine room which increases risk.

Ray: If this works, we can put RODC in Cambridge if it makes sense.
Dave H: Remote sites with bad data connections, that's where RODC typically helps.
Jim: Having a DC in remote sites is for catastrophic issues like link to main site down. I support that.
Dave A: Erick sent to us debug logs with user not found, no domain trust, no password server found. That happened for a 24-hour period during one day in March and we haven't seen this ever happening again. Looks as a transient network issue or failure. We don't know exactly what caused it because we haven't seen it since.
Dave A: RODC is a solution for a problem we're yet to define. The problem is likely to happen when right conditions or load occurs.
Ray: We're eliminating the firewall with RODC.

Allan: When we moved one of our systems into private subnet, we had a latency problem. Moving to public subnet helped to solve it.
Jim: We had some users having issues with private addresses as well, putting them in public solved the problem.
Dave H: If there were new subnets added in private, we have to know about this and edit the firewall rules on DCs to allow traffic.
Jim: The earlier problems with private addresses were intermittent.
Dave A: If anyone runs into same problem again - let us know and we will look into this.
Jim: As admins, we have to report problems in, so we can have a track of the problems. Going back to network drives disconnects – when we were doing this with old GPOs, we had the same experience. Solution was to re-do GPOs.

Jim: Did you get a specific error?
Dave H: We have only seen two errors – one from Erick and one from Hon's machine. We haven't seen any other errors from other machines. Erick says it happens 10% of time, but we have nothing else to look at aside from Erick and Hon's logs, nothing else.
Jim: Again, we're willing to help and do more tests to be able to point out the problem.
Lowell: I'm concerned about the time and resources we're putting into something we don't have enough details on in general.
Jim: Valid point. I would say that there some politics (from more than one group) slowing down collaborations. If we can't solve that, it should to be talked at the higher level. We are not collaborating as we used to and it is stopping progress. I'm willing to help if you want me to. If not, tell me and I'll leave it to you.

Jim: New topic: about smb1 issue… We have firewall rules put in place so not really at risk. Also, some patched machines still come out as vulnerable when IST was testing.
Mike: If you see some servers reporting errors or crashing – sorry, it's our tool doing scanning for vulnerabilities.
Jim: We have a small subset of machines that would not stop using smb1 for unknown reason. I think it's a case of an earlier patch from Microsoft that made things less stable. Re-enabled smb1 then disable it again and reboot (up to 3 times) and they are fine.
Manfred: We have seen such machines as well.
Jim: Our netapp is a weak point, can't have smb1 blocked or disabled separately. Different stack, hopefully not vulnerable. Waiting for NetApp to address.

Hard stop at this point as the battery on my laptop died…