NETWORK CREDENTIAL MANAGEMENT

BLOG POST 1: SO IT BEGINS...

SAM BREJCHA
@SAMBREJCHA
NOVEMBER 2016

There is a lot of talk in the world today about the attacks that happen in corporate America. Most (if not all) of these events have involved adversaries stealing network credentials. When compromising a network, adversaries will use a combination of different stolen network accounts to gain deeper access into your domain.

Let me illustrate the common scenario that happens all too often during these attacks:

Step 1: Adversary compromises a machine in the network and gains system access

Step 2: Adversary steals account credentials from the compromised machine while performing other reconnaissance activities

Step 3: Adversary repeats Step 2 until they steal an account that will allow them to move laterally to another system or grant more privileged access to the network (locked down file shares, websites to sensitive information, etc…)

Step 4: Adversary moves laterally to another system

Adversary repeats Steps 1 through 4 until they gain complete administrative control of the network or access to their target goal (credit card database, confidential files, intellectual property etc…).

These four steps are the standard playbook for most hackers and penetration test teams. I am highlighting this because this is THE tactic when attacking a network, yet network administrators are at a loss on how to combat this tactic. In a world where most IT staffs are overworked with an endless to-do list, credential management is the last thing they even want to consider. To do so correctly on an already established network, formalizing a credential risk mitigation program is an uphill battle that entails not only changing technical configurations but corporate culture as well. It is easier to use default security controls and remote management for everything in the network, especially with organizations that have geographically separate locations, and require remote management. This requirement for remote management opens up avenues for the above scenario to play out time and time again. So what is the answer? Where is the middle ground between security and availability? Well, we here at root9B have an answer.

Well, not an answer, but a series of answers. When it comes to credential management, there is no "silver bullet." In fact, I believe a term in this context is counterproductive. Bullets are most often used in offensive engagements. What we want is some type of defense or shield against credential theft. To help you out, we will be creating a series of blog posts to provide small things that IT departments can implement to build their defensive strategy for credential management. We will explore simple, but powerful counter measures that will frustrate attackers once they gain access to your network. To be honest, you must assume you are compromised or that you will be compromised. An employee will click a link that will download malware to allow the adversary's inside your network. Our goal in this series is to provide actionable advice that reduces the adversary's ability to get further into your network, forcing them to give up before you catch them. The only cost of this series is time and effort.

I am looking forward in providing great ways for administrators to help clean and harden their networks. Stay tuned for our first topic post on Credential Management: “The Pyramids of Delegation Models.”

ABOUT ROOT9B

Ranked as the #1 Cybersecurity company for three consecutive quarters by Cybersecurity Ventures (Jan 2016), root9B stands in defiance of the unwanted human presence within our clients’ networks by attacking the root of the problem—the adversary’s ability to gain entry and remain undetected. root9B’s application of advanced technology developed through cutting-edge R&D and engineering and refined through relevant, hands-on training is revolutionary. root9B combines cutting-edge technology, tactics development, specialty tools, and deep mission experience. root9B personnel leverage their extensive backgrounds in the U.S. Intelligence Community to conduct advanced vulnerability analysis, penetration testing, digital forensics, incident response, Industrial Control System (ICS) security, and active adversary pursuit (HUNT) engagements on networks worldwide. For more information, visit www.root9B.com.

WWW.ROOT9B.COM