Real-World Example of How Active Directory Can Be Compromised (RSA Conference Presentation)

adsecurity.org

Sean Metcalf

November 30, 2015

At the RSA Conference in Abu Dhabi earlier this month, Stefano Maccaglia (Incident Response Consultant with RSA) presented “Evolving Threats: dissection of a Cyber-Espionage attack.” The slides for this talk are available on the RSA Conference site (*UPDATE: RSA removed the slides from their site, Presentation Slides on Yumpu*). This post covers and adds some additional detail to the attack that Stefano Maccaglia and RSA colleagues dealt with as described in this talk. I have no information about this attack other than what is covered in the slides since I wasn’t involved in the incident response. Since this RSA talk has great detail on the attack, I am taking the opportunity to point how what weaknesses the attacker exploited and how other organizations can learn from this breach. I don’t deal with attribution, so I leave it to the reader to follow the presenter’s narrative on who the attacker was.

The attack started, as many do, with a spear-phish email which was opened and code executed (in this case leveraging a Microsoft Word exploit). It is noted that the internet proxy blocked seven (7) out of nine (9) of the attacks. It only takes one success though for the attacker to gain a foothold inside the network. Note that there was a second wave which adjusted to the internet proxy configuration and was far more successful the second time around. Always expect that the attacker will quickly learn more about your environment than what you have documented.
I don’t cover malware, so I won’t dig into the details of what the code did other than recon, privilege escalation, and lateral movement.

It is interesting that the attacker leveraged OWA to use stolen credentials to spread the malware using internal email addresses. The benefit to the attacker is that users often are more likely to open websites and files sent from internal email addresses.

The other interesting part is that the attacker also leveraged SharePoint to expand access by distributing the malware further. Is your organization checking for malware in SharePoint? You should.
Once the attacker has access to commonly accessed/downloaded data, any of it can be updated with malware to either expand access or persist.

Active Directory:

The Active Directory forest is described as having a root domain with three (3) child domains and it is noted that the AD forest is the administrative boundary. This is an important distinction since many people still believe that the AD domain is the admin/security boundary (which isn’t true). This belief often leads to rapid forest compromise since a single domain configured with weak security can lead to compromising the entire AD forest. Based on the presentation slides, this seems to be how this occurred. There is a statement regarding the forest is “regulated with different level of trust.” This may mean that one of the child domains was not secured to the same level as the others.

Additionally, the presentation notes that the network is segmented, but the IDS/IPS was not configured to properly monitor traffic on the internal network to identify attackers inside the system. This is an issue with the majority of customers I speak with about network security.

The environment described in the RSA Conference talk states that systems are patched 15 days after Microsoft releases the patches.The presentation states “During the investigation we have discovered that, in the Data Center, two AD servers related to trusted subdomains, were not properly patched since November 2014 due to the swap from a maintenance contractor to another. The lack of the patch MS14-068 is a key to understand how deep and how hard they have been breached” Assuming the unpatched systems were Domain Controllers, this means the attacker could exploit the MS14-068 vulnerability to easily escalate rights from domain user to domain admin in about 5 minutes. The slides describe that two child domains had these issue, though full forest compromise is possible due to a single Domain Controller unpatched for MS14-068.

It is likely that once the attacker identified a Domain Controller was unpatched for MS14-068, it is a simple matter to go from Domain User to Domain Admin. One of the screenshots in the presentation shows Event ID 4624, “an account was successfully logged on,” showing the security ID and account name don’t match. Once a single domain in an AD forest is compromised, it doesn’t take much to compromise the other domains in the forest.

Active Directory Exploit Process:

- The attacker gains control of a number of domain user accounts (from spearphshing and spread of malware).
- Network activity is speculative due to lack “of logs and network visibility.”
- *‘AD servers are breached, has collected domain admins credentials and has moved forward to the Root AD and the repositories where “interesting data” resides.’*
- Mimikatz was used, though there are no details as to which components were used. My guess is that Mimikatz was used to dump credentials, dump the AD domain databases, create and use Golden Tickets, etc.

Practical Defense Against this Type of Attack:

- Rapidly Patch all Domain Controllers with critical patches and regularly check to ensure they are installed. DCs get rebuilt from time to time.
- Ensure that internal network traffic is monitored using IDS, NetFlow, or other.
- Ensure that security logs flow to a central logging system to identify anomalies.

- Digitally sign internal email. The attacker could extract the private key for signing email, but this limits how the attacker interacts with the system. Unsigned email from internal senders should be considered suspect.
- Remember that notification of an attack, even if blocked, is as important as blocking the attack in the first place. This presentation noted that the attacker was only partly successful with the first wave of spearphishing, so they adapted. Without visibility of the first attack, it may be difficult to associate to the second.

NOTE:
This post is my interpretation of a presentation from the RSA Conference in Abu Dhabi based on the slides published on RSA's website. I don't have any more information on what happened beyond what is in the slides and I didn't see the presentation, so I don't know what was said during the talk.
Thanks Tal Be'ery for tweeting about it or I would have likely missed it.

References:

(Visited 5,042 times, 1 visits today)