Reversing Malware How is APT 29 Successful w/ this Phishing Tech and BRc4 (Brute Ratel) opsec fails?

Published: 2022-07-05 · Archived: 2026-04-05 14:29:18 UTC

00:00 - Introduction, talking about why I think APT-29 successfully phishing is funny 01:10 - Unit42's blog post talking about how the phishing document worked 02:15 - Going to google to show APT29 doing the lnk file in a zip since atleast 2016, Mandiant post. 03:40 - Talking about why phishers put executables or things to click on in zip/iso/compressed folders 04:50 - Talking about why they may use DLL Side Loading to execute the shellcode 06:25 - Showing what the user see's when they open the iso file 07:48 - Talking about why we are starting with shellcode instead of a weaponized document and why red teams like shellcode 09:00 - Using MSFVenom to generate a malicious executable with custom shellcode from BRc4 10:15 - Opening the executable with x64dbg, so we can extract a program from memory. This is great for when the shellcode is obfuscated through like shikata ga nai 11:00 - Setting a breakpoint on LdrLoadDll, showing the memory map is empty 12:15 - Running the program, examining memory on LdrLoadDll breakpoint. Showing a weird Execute-Read Permission, which initially was Read-write (screwed up initially explaining it) 13:10 - The E_MAGIC (MZ Header) is nulled out, talking about why the brute ratel may do that 14:20 - Dumping the memory to a file, copying it to linux where i have ida 15:30 - Using hexedit to set the first two bits to MZ, so ida recognizes it as an executable 16:50 - Talking about ordinal loading 18:05 - Showing the applicaiton uses ror13 hashes to call functions to avoid strings. Using google to find what the hash goes to 20:20 - The coffee string is weird, going into it 21:10 - Looking at a function that looks like it sends strings to the teamserver 22:45 - Showing similarities of the coff loader from trusted sec 24:00 - Converting another ror13 hash in badger to a function 25:25 - Having ida show all strings 25:50 - Looking at the AMSI Patch thing 26:35 - Stumbling across a static encryption key 29:00 - Looking at a likely PSExec functionality, maybe an IOC? Service name: ServicesActive 36:15 - Looking at the EnableDebug command and explaining why i think all these strings may be in the binary right now, they are likely gone now.

Så skapades det här

Automatiskt dubbad

Ljudspår har genererats automatiskt för vissa språk. Läs mer

Source: https://www.youtube.com/watch?v=a7W6rhkpVSM