Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:27:52 UTC

Tool: SkeletonKeyInjector

Names	SkeletonKeyInjector
Category	Malware
Type	Backdoor
Description	(CyCraft) The discovery of a related binary led us to initially believe the sample was a Dumpert. However, a more in-depth analysis revealed that the d3d11.dll sample implanted a skeleton key, where adversaries could persistently control (before the system reboot) the infected machine and machines under the infected AD. More specifically, the malware was an account manipulation tool that contained code extracted from both Dumpert and Mimikatz. We called this malware SkeletonKeyInjector. The malware employed a technique that altered the NTLM authentication program and implanted a skeleton key to allow adversaries to log-in without a valid credential. This allowed the adversary to achieve the following objectives: ● Persistence: After the code in memory was altered, the adversary could gain access to the compromised machines before the next system reboot. As AD machines are rarely rebooted, the adversary was able to control the machines for a very long time. ● Defense Evasion: Aside from the different login password and login algorithm scheme, there was no difference when compared to a normal login activity. Furthermore, normal users could still log-in to the system via their original password. Thus, the probability of being exposed was low. ● Lateral Movement: Adversaries could use the skeleton key to login to other machines that were in the same domain. This made it easier for an adversary to conduct lateral movement.
Information	<https://cycraft.com/download/%5BTLP-White%5D20200415%20Chimera_V4.1.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool SkeletonKeyInjector

Changed	Name	Country	Observed

APT groups

	Chimera		2018-Oct 2019	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ac256455-69de-4b40-9ca5-bb207aaf5b08