

LetsDefend: Lockbit

The following writeup is for [LockBit](#) on LetsDefend, it involves investigating a memory dump using volatility.

Scenario: You are a Digital Forensics and Incident Response (DFIR) analyst tasked with investigating a ransomware attack that has affected a company's system. The attack has resulted in file encryption, and the attackers are demanding payment for the decryption of the affected files. You have been given a memory dump of the affected system to analyse and provide answer to specific questions related to the attack.

Can you determine the date and time that the device was infected with the malware? (UTC, format: YYYY-MM-DD hh:mm:ss)

We first need to identify the malicious process, so I am going to start off by listing network connections and see if any process was communicating with a foreign IP address (likely indicative of C2 activity). We can do so by using the windows.netscan plugin. Unfortunately this didn't provide anything useful, so let's use the psscan plugin:

```
vol -f Lockbit.vmem windows.psscan
```

```
900      216      mal.exe 0x7fdccb00      267      1254      1      True      2023-04-13 10:06:45.000000
```

mal.exe is obviously the malicious process, meaning the answer is 2023-04-13 10:06:45.

What is the name of the ransomware family responsible for the attack?

The answer is obviously lockbit based on the name of the challenge, however, let's assume that we aren't given the name. We can use the psslist plugin to dump the process, use sha256sum to generate the hash of the file, and enter it into VirusTotal:

```
vol -f Lockbit.vmem windows.pslist --pid 900 --dump
```

```
sha256sum 900.mal.exe.0x400000.dmp
```

```
55f5115538984e74eedcd0aa2edbede4381dd85e57f26bae71fc348039b35050 900.mal.exe.0x400000.dmp
```


Note! It seems as if dumping the process is not the intended way to answer the questions. Therefore, I used the dumpfiles plugin followed by the process ID of the malicious process:

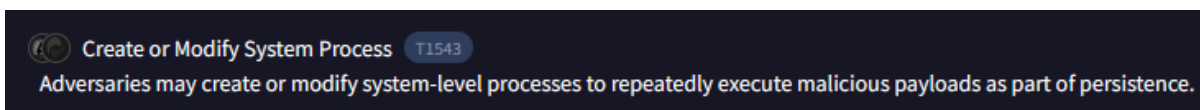
```
vol -f Lockbit.vmem windows.dumpfiles --pid 900
```

```
0xfa801bfe5320 mal.exe file.0xfa801bfe5320.0xfa801bde2b10.DataSectionObject.mal.exe.dat  
0xfa801bfe5320 mal.exe file.0xfa801bfe5320.0xfa801c116990.ImageSectionObject.mal.exe.img
```

We are most concerned with the .dat file, so hash this file and enter it into VirusTotal to get the answer.

Which MITRE ATT&CK technique ID was used by the ransomware to perform privilege escalation?

You can find the technique used for privilege escalation in the behaviour tab:



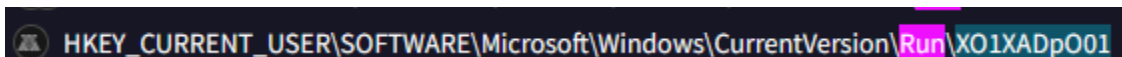
Create or Modify System Process T1543
Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence.

What is the SHA256 hash of the ransom note dropped by the malware?

You can find the sha256 hash of the ransom note in the files dropped section on VirusTotal:

67c6784a5296658ac4d633f4e8c0914ecc783b1cf2f6431818c4e2f3cdcce91f

What is the name of the registry key edited by the ransomware during the attack to apply persistence on the infected system?



HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run XO1XADpO01

There are multiple ways to do this, however, the easiest is to just look at the Registry Actions section in the behaviour tab on VirusTotal.