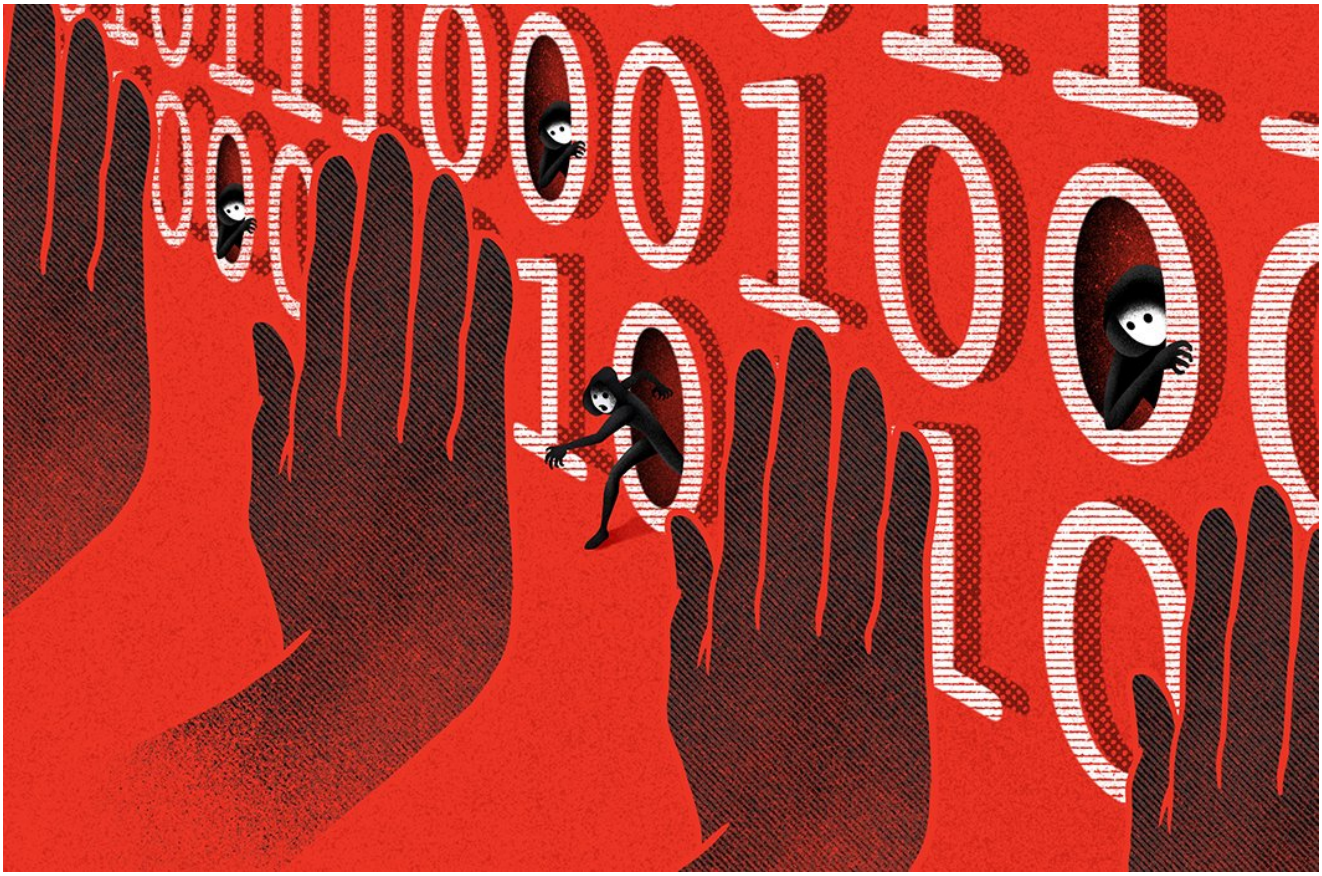
How CrowdStrike Prevents Volume Shadow Tampering by LockBit

crowdstrike.com/blog/how-crowdstrike-prevents-volume-shadow-tampering-by-lockbit-ransomware/

Thomas Moses - Sarang Sonawane - Liviu Arsene November 17, 2021



- ECrime activities dominate the threat landscape, with ransomware as the main driver
- Ransomware operators constantly refine their code and the efficacy of their operations
- CrowdStrike uses improved behavior-based detections to prevent ransomware from tampering with Volume Shadow Copies
- Volume Shadow Copy Service (VSS) backup protection nullifies attackers' deletion attempts, retaining snapshots in a recoverable state

Ransomware is dominating the eCrime landscape and is a significant concern for organizations, as it can cause major disruptions. ECrime accounted for over 75% of interactive intrusion activity from July 2020 to June 2021, according to the recent CrowdStrike 2021 Threat Hunting Report. The continually evolving big game hunting (BGH) business model has widespread adoption with access brokers facilitating access, with a major driver being dedicated leak sites to apply pressure for victim compliance. Ransomware continues to evolve, with threat actors implementing components and features that make it more difficult for victims to recover their data.

Lockbit 2.0 Going for the Popularity Vote

The LockBit ransomware family has constantly been adding new capabilities, including tampering with Microsoft Server Volume Shadow Copy Service (VSS) by interacting with the legitimate vssadmin.exe Windows tool. Capabilities such as lateral movement or destruction of shadow copies are some of the most effective and pervasive tactics ransomware uses.

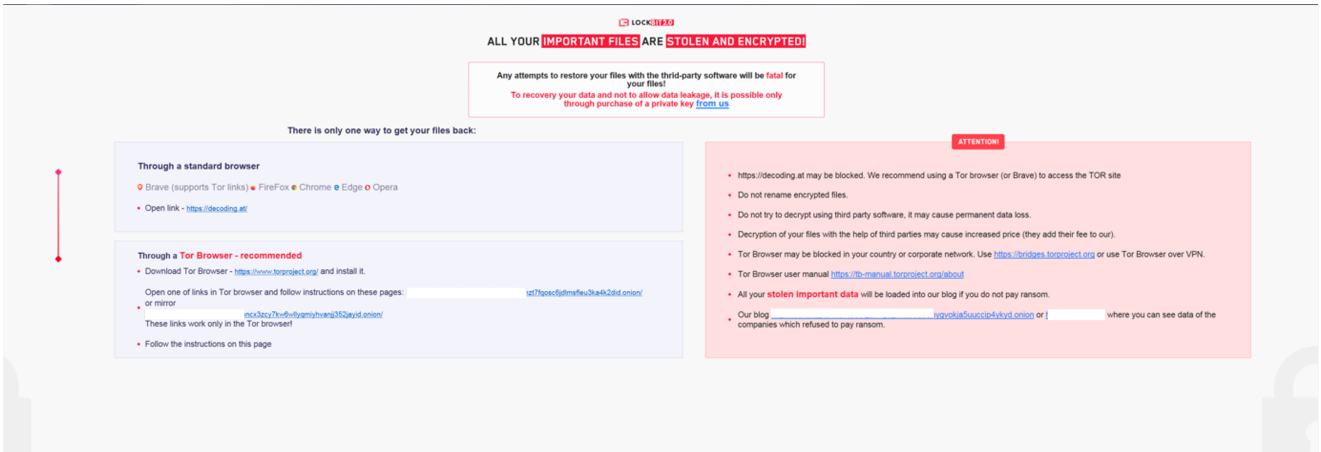


Figure 1. LockBit 2.0 ransom note (Click to enlarge)

The LockBit 2.0 ransomware has similar capabilities to other ransomware families, including the ability to bypass UAC (User Account Control), self-terminate or check the victim's system language before encryption to ensure that it's not in a Russian-speaking country.

For example, LockBit 2.0 checks the default language of the system and the current user by using the Windows API calls `GetSystemDefaultUILanguage` and `GetUserDefaultUILanguage`. If the language code identifier matches the one specified, the program will exit. Figure 2 shows how the language validation is performed (function call `49B1C0`).

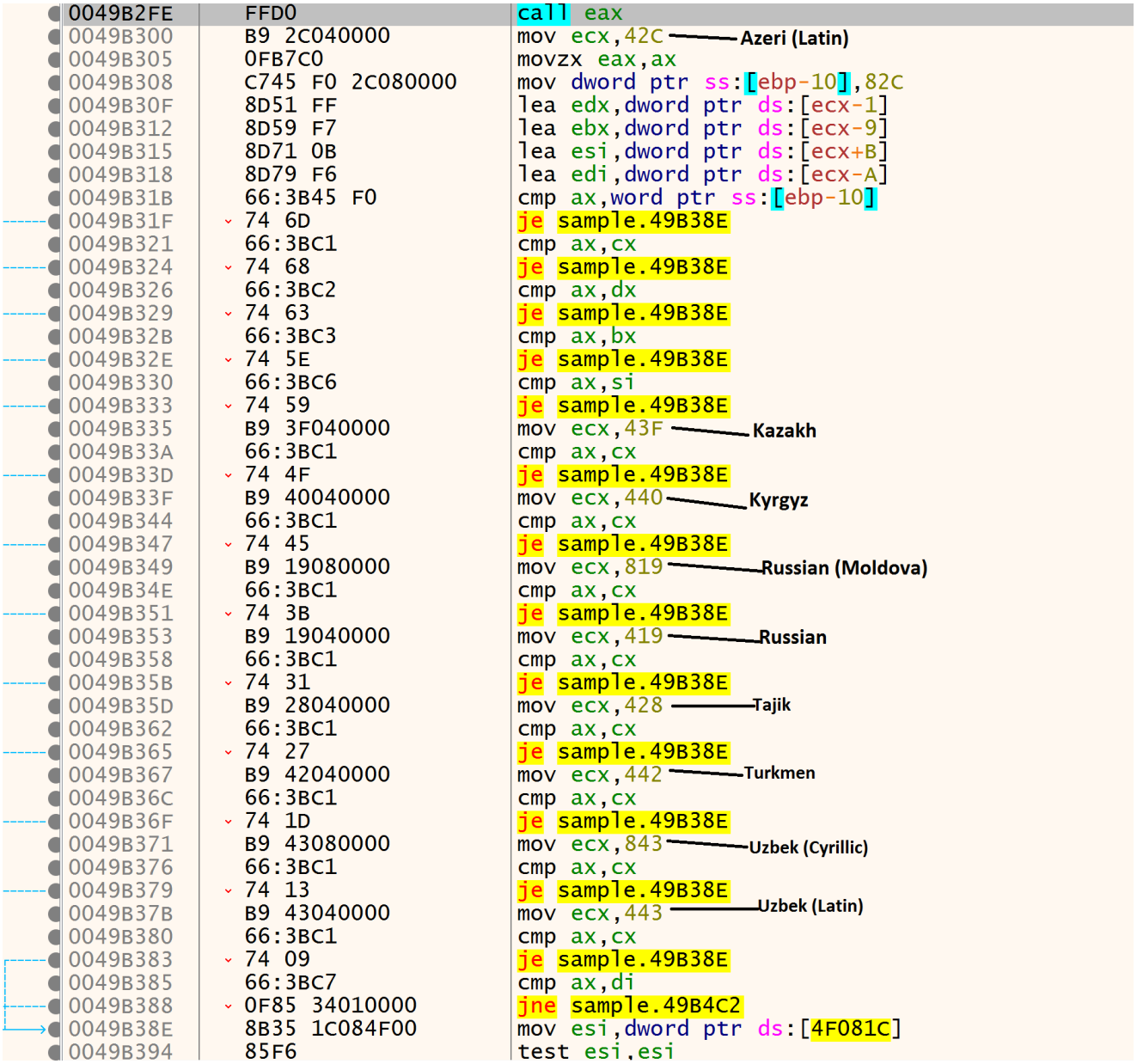


Figure 2. LockBit 2.0 performing system language validation

LockBit can even perform a silent UAC bypass without triggering any alerts or the UAC popup, enabling it to encrypt silently. It first begins by checking if it's running under Admin privileges. It does that by using specific API functions to get the process token (`NTOpenProcessToken`), create a SID identifier to check the permission level (`CreateWellKnownSid`), and then check whether the current process has sufficient admin privileges (`CheckTokenMembership` and `ZwQueryInformationToken` functions).

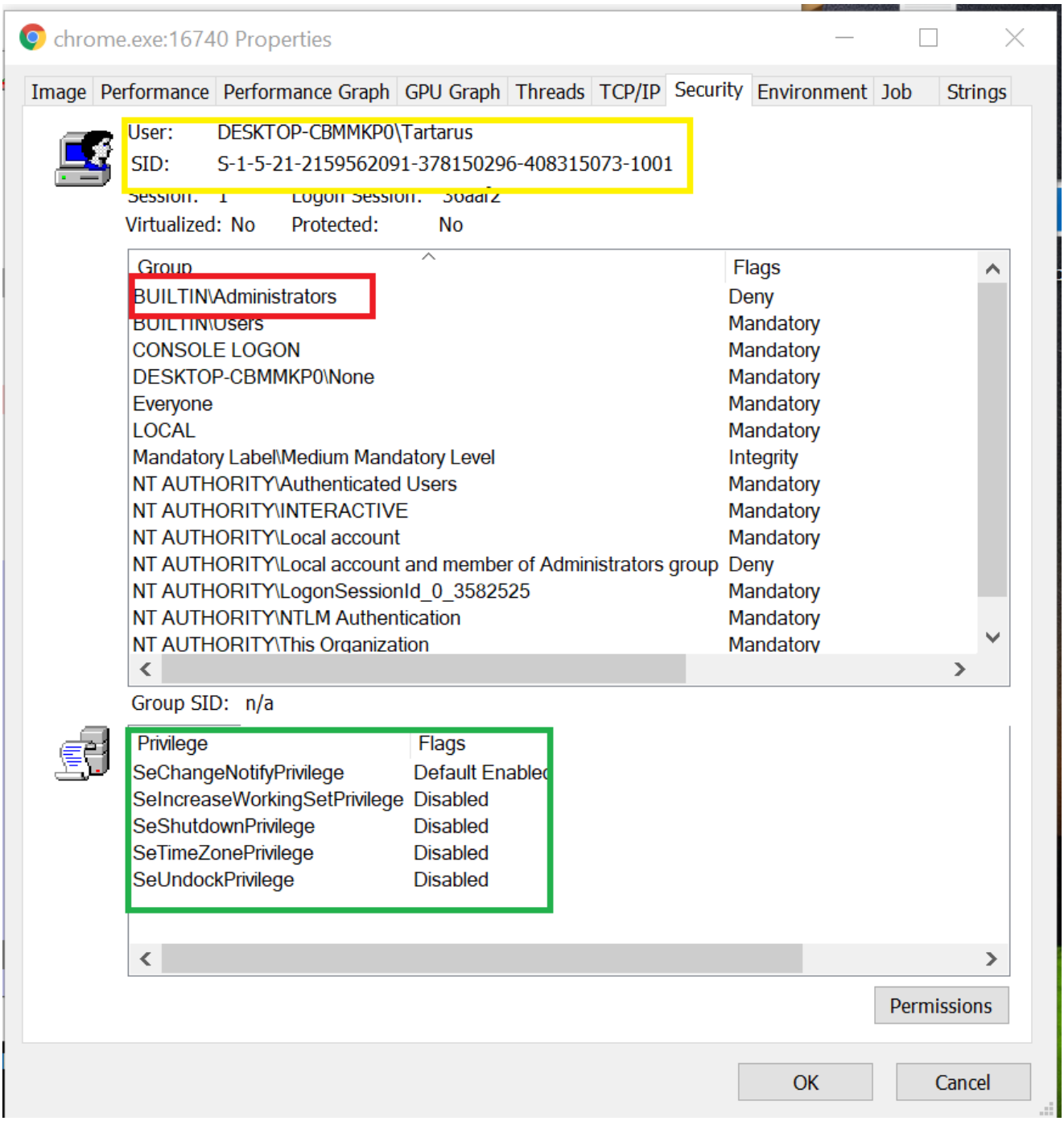


Figure 3. Group SID permissions for running process

If the process is not running under Admin, it will attempt to do so by initializing a COM object with elevation of the COM interface by using the elevation moniker COM initialization method with guid: `Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}`. A similar elevation trick has been used by DarkSide and REvil ransomware families in the past.

LockBit 2.0 also has lateral movement capabilities and can scan for other hosts to spread to other network machines. For example, it calls the `GetLogicalDrives` function to retrieve a bitmask of currently available drives to list all available drives on the system. If the found

drive is a network share, it tries to identify the name of the resource and connect to it using API functions, such as `WNetGetConnectionW`, `PathRemoveBackslashW`, `OpenThreadToken` and `DuplicateToken`.

In essence, it's no longer about targeting and compromising individual machines but entire networks. REvil and LockBit are just some of the recent ransomware families that feature this capability, while others such as Ryuk and WastedLocker share the same functionality. The CrowdStrike Falcon OverWatch™ team found that in 36% of intrusions, adversaries can move laterally to additional hosts in less than 30 minutes, according to the CrowdStrike 2021 Threat Hunting Report.

Another interesting feature of LockBit 2.0 is that it prints out the ransom note message on all connected printers found in the network, adding public shaming to its encryption and data exfiltration capabilities.

VSS Tampering: An Established Ransomware Tactic

The tampering and deletion of VSS shadow copies is a common tactic to prevent data recovery. Adversaries will often abuse legitimate Microsoft administrator tools to disable and remove VSS shadow copies. Common tools include Windows Management Instrumentation (WMI), BCDEdit (a command-line tool for managing Boot Configuration Data) and vssadmin.exe. LockBit 2.0 utilizes the following WMI command line for deleting shadow copies:

```
C:\Windows\System32\cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no
```

The use of preinstalled operating system tools, such as WMI, is not new. Still, adversaries have started abusing them as part of the initial access tactic to perform tasks without requiring a malicious executable file to be run or written to the disk on the compromised system. Adversaries have moved beyond malware by using increasingly sophisticated and stealthy techniques tailor-made to evade autonomous detections, as revealed by CrowdStrike Threat Graph®, which showed that 68% of detections indexed in April-June 2021 were malware-free.

VSS Protection with CrowdStrike

CrowdStrike Falcon takes a layered approach to detecting and preventing ransomware by using behavior-based indicators of attack (IOAs) and advanced machine learning, among other capabilities. We are committed to continually improving the efficacy of our technologies against known and unknown threats and adversaries.

CrowdStrike's enhanced IOA detections accurately distinguish malicious behavior from benign, resulting in high-confidence detections. This is especially important when ransomware shares similar capabilities with legitimate software, like backup solutions. Both can enumerate directories and write files that on the surface may seem inconsequential, but when correlated with other indicators on the endpoint, can identify a legitimate attack. Correlating seemingly ordinary behaviors allows us to identify opportunities for coverage across a wide range of malware families. For example, a single IOA can provide coverage for multiple families and previously unseen ones.

CrowdStrike's recent innovation involves protecting shadow copies from being tampered with, adding another protection layer to mitigate ransomware attacks. Protecting shadow copies helps potentially compromised systems restore encrypted data with much less time and effort. Ultimately, this helps reduce operational costs associated with person-hours spent spinning up encrypted systems post-compromise.

The Falcon platform can prevent suspicious processes from tampering with shadow copies and performing actions such as changing file size to render the backup useless. For instance, should a LockBit 2.0 ransomware infection occur and attempt to use the legitimate Microsoft administrator tool (vssadmin.exe) to manipulate shadow copies, Falcon immediately detects this behavior and prevents the ransomware from deleting or tampering with them, as shown in Figure 4.

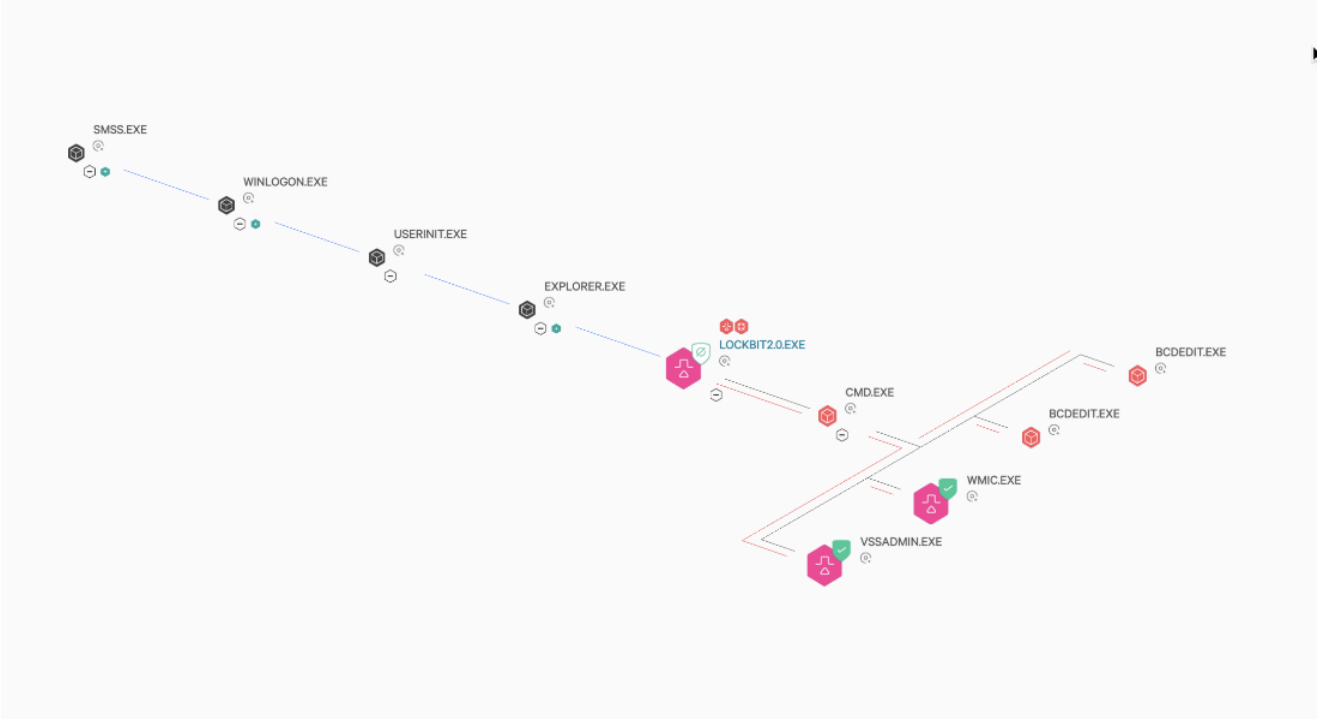


Figure 4. Falcon detects and blocks vssadmin.exe manipulation by LockBit 2.0 ransomware (Click to enlarge)

In essence, while a ransomware infection might be able to encrypt files on a compromised endpoint, Falcon can prevent ransomware from tampering with shadow copies and potentially expedite data recovery for your organization.

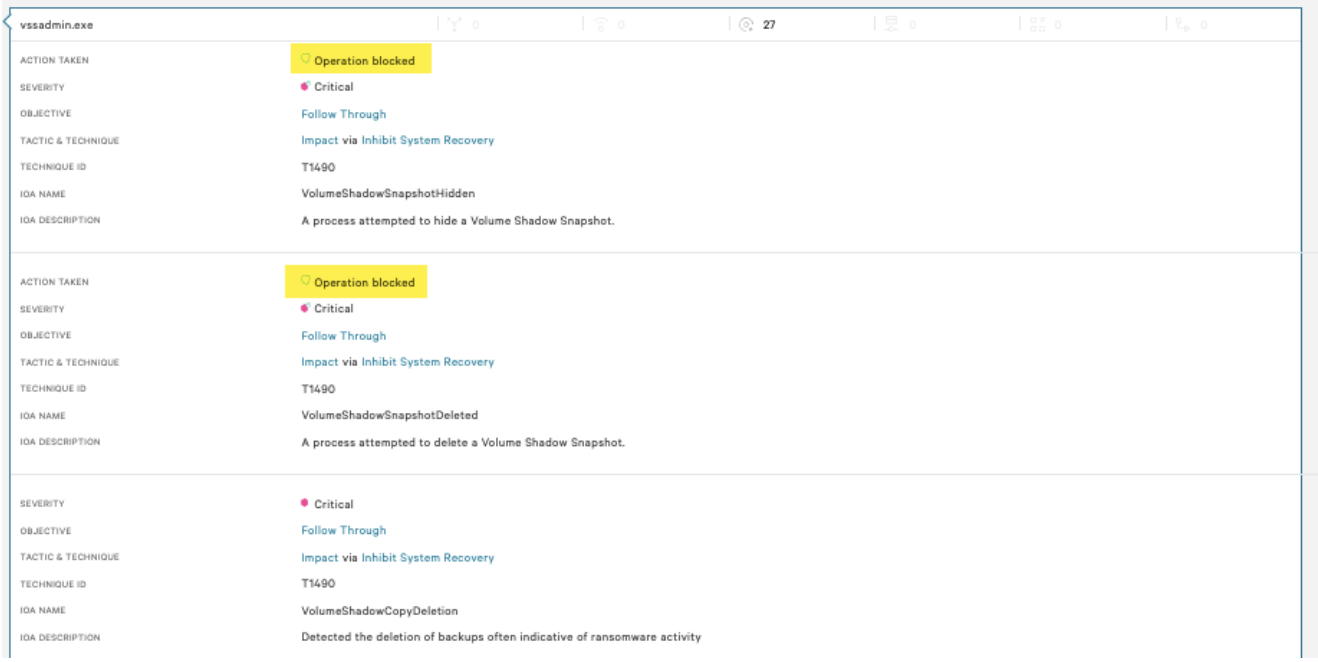
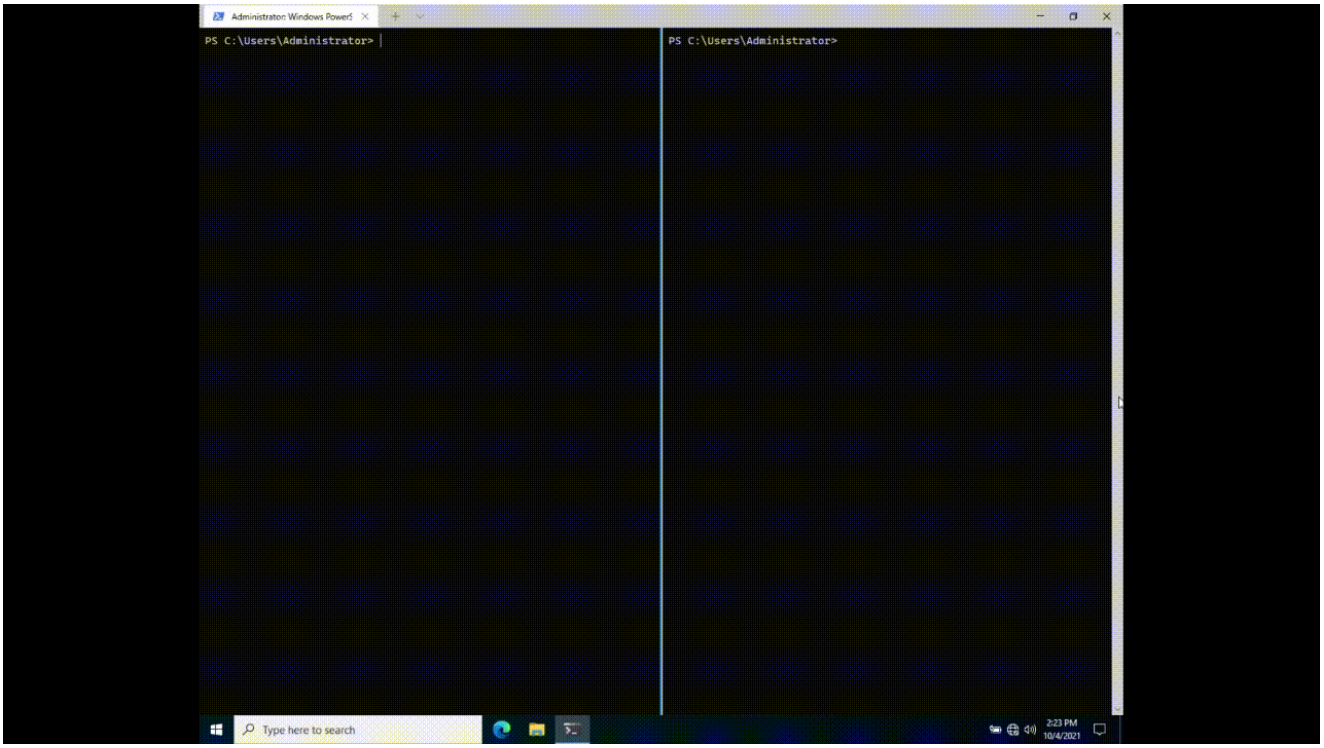


Figure 5. Falcon alert on detected and blocked ransomware activity for deleting VSS shadow copies (Click to enlarge)

Shown below is Lockbit 2.0 executing on a system without Falcon protections. Here, vssadmin is used to list the shadow copies. Notice the shadow copy has been deleted after execution.



Below is the same Lockbit 2.0 execution, now with Falcon and VSS protection enabled. The shadow copy is not deleted even though the ransomware has run successfully. Please note, we specifically allowed the ransomware to run during this demonstration.

CrowdStrike prevents the destruction and tampering of shadow copies with volume shadow service backup protection, retaining the snapshots in a recoverable state regardless of threat actors using traditional or new novel techniques. This allows for instant recovery of live systems post-attack through direct snapshot tools or system recovery.

VSS shadow copy protection is just one of the new improvements added to CrowdStrike's layered approach. We remain committed to our mission to stop breaches, and constantly improving our machine learning and behavior-based detection and protection technologies enables the Falcon platform to identify and protect against tactics, techniques and procedures associated with sophisticated adversaries and threats.

CrowdStrike's Layered Approach Provides Best-in-Class Protection

The Falcon platform unifies intelligence, technology and expertise to successfully detect and protect against ransomware. Artificial intelligence (AI)-powered machine learning and behavioral IOAs, fueled by a massive data set of trillions of events per week and threat actor intelligence, can identify and block ransomware. Coupled with expert threat hunters that proactively see and stop even the stealthiest of attacks, the Falcon platform uses a layered approach to protect the things that matter most to your organization from ransomware and other threats.

CrowdStrike Falcon endpoint protection packages unify the comprehensive technologies, intelligence and expertise needed to successfully stop breaches. For fully managed detection and response (MDR), Falcon Complete™ seasoned security professionals deliver 403% ROI and 100% confidence.

Indicators of Compromise (IOCs)

File	SHA256
LockBit 2.0	`0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049`

Additional Resources

- *Learn more about ransomware adversaries in the CrowdStrike Adversary Universe.*
- *Download the CrowdStrike 2021 Global Threat Report for more information about adversaries tracked by CrowdStrike Intelligence in 2020.*
- *See how the powerful, cloud-native CrowdStrike Falcon® platform protects customers from the latest variants of ransomware in these blogs: DarkSide Goes Dark: How CrowdStrike Falcon Customers Were Protected and Under Attack: Protecting Against Conti, DarkSide, REvil and Other Ransomware.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*