DTEX

THE WORKFORCE CYBER INTELLIGENCE COMPANY™

DTEX CUSTOMER THREAT ADVISORY

SOLARWINDS SUPPLY CHAIN ATTACK

This DTEX Threat Advisory provides practical advice for DTEX customers to:

1. **CONFIRM** – Produce an evidentiary audit trail that confirms critical server environments have not been impacted
2. **DETECT** – Identify the presence of affected SolarWinds products on your servers and connected endpoints
3. **IMPACT** – Assess potential impact using the MITRE ATT&CK and DTEX C-InT Frameworks
4. **MONITOR** – Know how to use DTEX InTERCEPT to continuously monitor superuser account behaviors and behavioral signs of a breach

DTEX C-InT INSIGHTS

DTEX is continuing to follow the SolarWinds Supply Chain Cyberattack, as detailed in this recent Security Advisory. While the DTEX Workforce Cyber Intelligence Platform™ nor our cloud-infrastructure has not been directly impacted by the breach, we have received numerous requests from DTEX customers for assistance in reviewing existing endpoint and **server environments** for behavioral indicators, which include:

- Inventory of assets executing **impacted SolarWinds products**
- **Account compromise behaviors** associated with this or similar breaches
- Contextualization of the **impact** (what was accessed, when and why)

The following threat advisory provides practical examples of how DTEX InTERCEPT™ can and should be leveraged, along with the introduction of a new dashboard that summarizes TTPs, which may indicate suspicious activity associated with these events.

WHAT DO WE KNOW ABOUT THE ATTACK?

As reported by cybersecurity firm FireEye, hackers inserted "*malicious code into legitimate software updates for the SolarWinds Orion software that allow an attacker remote access into the victim's environment*" with reported "*indications of compromise dating back to the spring of 2020*." The attack reportedly leveraged a backdoor in a SolarWinds library, which was initiated when an update to SolarWinds was applied. Subsequently, it has become apparent that multiple government agencies, in addition to FireEye, have been breached by this historical attack vector[1].

HOW CAN DTEX HELP?

While DTEX InTERCEPT™ is not typically utilized as a first line of defense against such attacks, the nature of this attack suggests **behavioral profiling of superuser accounts**. Traditional cyber defense methods fall short and do not provide visibility of these kill chain behaviors prior to a breach and customer exposure. The following attack observations detail the behaviors that were occurring, and may still be, within customer environments as a result of the SolarWinds Orion software attack:

- **Minimal malware:** Following the establishment of the backdoor, minimal malware TTPs were leveraged, making the attack vector difficult to detect via traditional means.
- **Stealth:** Significant attempts appear to have been made to avoid detection by blending into normal network activity (e.g., trusted certificates, etc.).
- **High reliance on typical administrative tools:** The attack appears to have had heavy reliance on difficult-to-attribute tools to conduct reconnaissance and cover tracks → hence the profiling of anomalous behavior of superuser accounts on affected endpoints and servers is paramount.

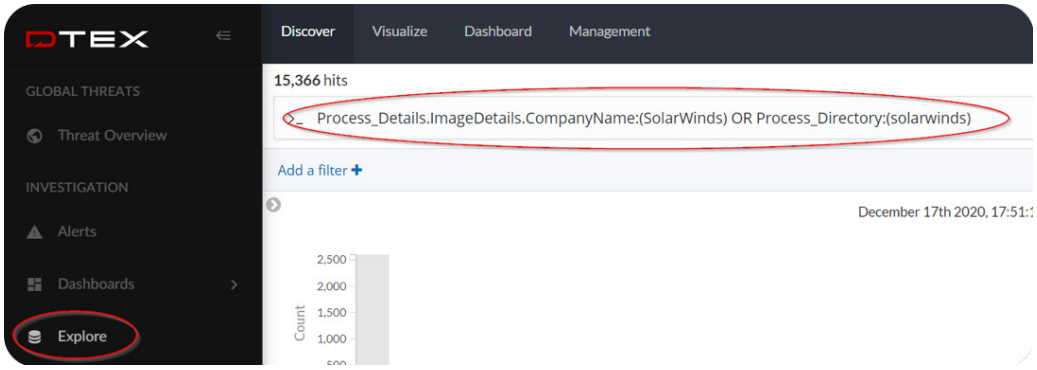
Below is a list of recommended steps to review the incident within your own DTEX environment.

1. https://www.nytimes.com/2020/12/16/us/politics/russia-hack-putin-trump-biden.html

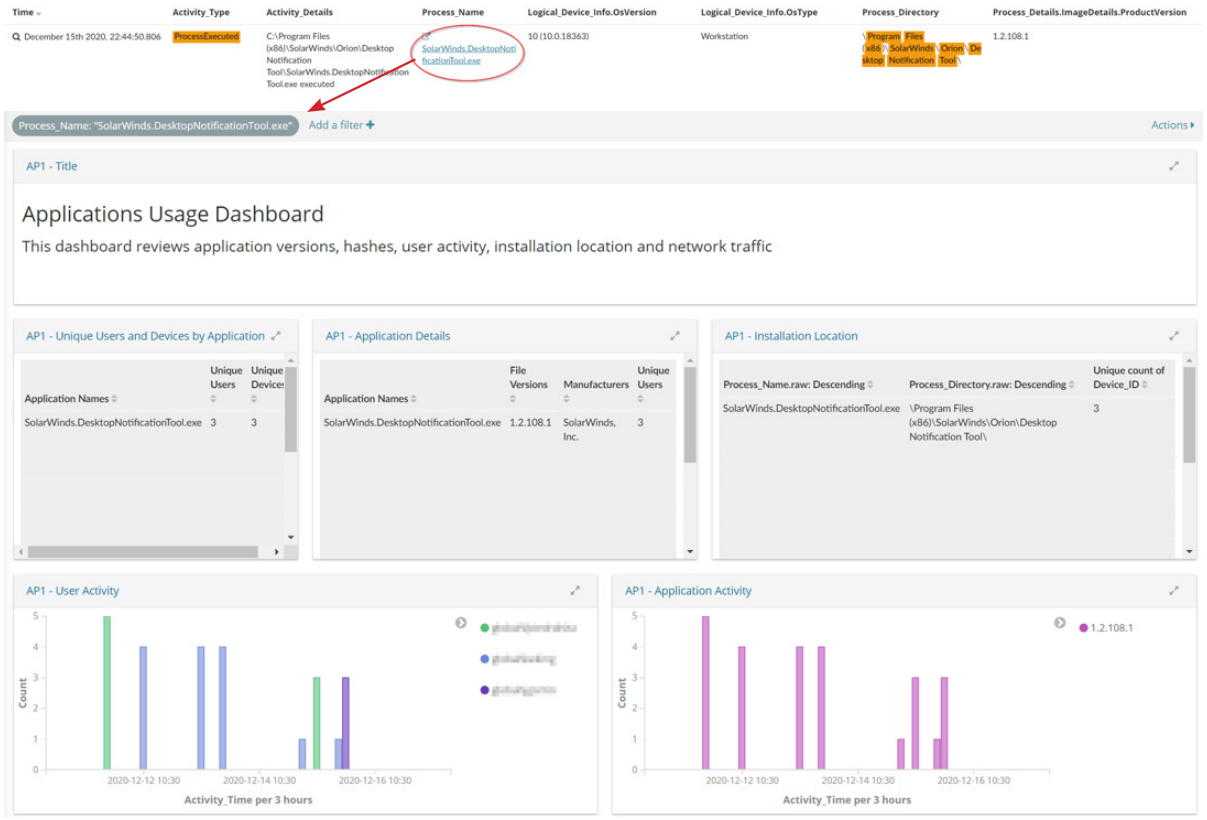
REVIEW STEP #1 – IDENTIFICATION OF ENDPOINTS & SERVERS EXECUTING SOLARWINDS PRODUCTS

Enter the following query in the DTEX 'EXPLORE' page to identify any endpoints or servers executing SolarWinds products:

Process_Details.ImageDetails.CompanyName:(SolarWinds) OR Process_Directory:(solarwinds)



Click on the 'Process_Name' link to review the full version details and all users, devices and network activity associated with the selected product:



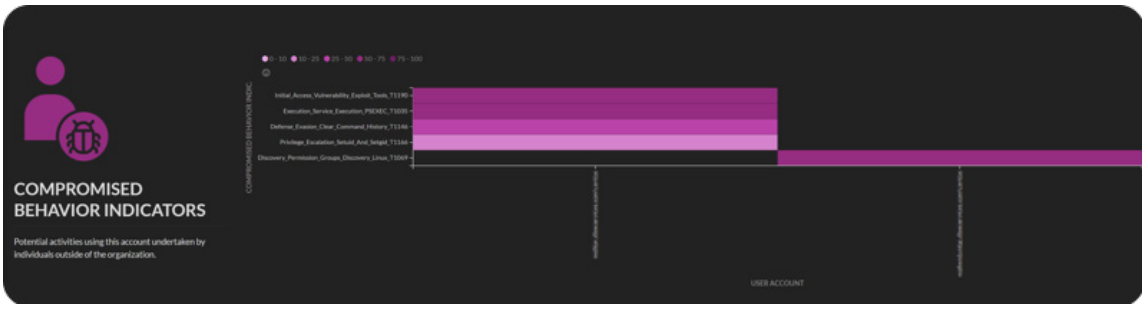
REVIEW STEP #2 – LINUX SERVER ENVIRONMENTS

Navigate to the 'ALERT HEAT MAP' and filter on any Linux User Accounts (User_Name), which have been identified in Step #1 above:

- Linux Device Query used to identify Linux servers in Step #1:

  Logical_Device_Info.OsPlatform:(Linux*)

Review any anomalous 'Compromised' behavior indicators for these devices:



REVIEW STEP #3 – WINDOWS SERVER ENVIRONMENTS

Navigate to the 'ALERT HEAT MAP' and filter on any Windows Server User Accounts (User_Name), which have been identified in Step #1 above:

- Windows Server Device Query used to identify Windows servers in Step #1:

  Logical_Device_Info.OsPlatform:(Windows) AND Logical_Device_Info.OsType:(Server)

Review any anomalous 'Compromised' behavior indicators for these devices as per Step #2.

REVIEW STEP #4 – WORKSTATION ENVIRONMENTS

Navigate to the 'ALERT HEAT MAP' and filter on any Windows Workstation User Accounts (User_Name), which have been identified in Step #1 above:

- Windows Workstation Device Query used to identify Windows endpoints in Step #1:

  Logical_Device_Info.OsPlatform:(Windows) AND Logical_Device_Info.OsType:(Workstation)

Review any anomalous 'Compromised' behavior indicators for these devices as per Step #2.

In addition to the above steps, it is prudent to identify all of the associated endpoint workstations that may have had access to the associated server environments. This can be identified using the following methods:

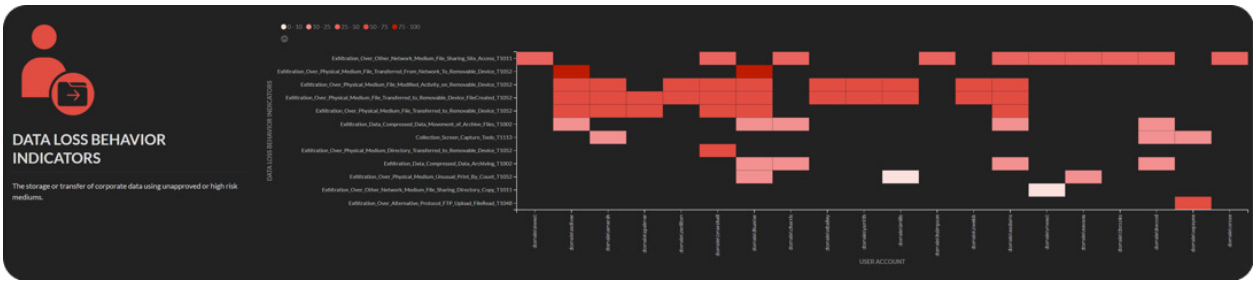
- Review any RDP Session Activities related to these server environments, taking note of the Remote_Host_Name values:

- Review domain user account access to these server environments and subsequent risk profiles for each user account (User_Name).
- Review network communications between workstations and servers with your environment using the Port_Accessed activity type.

REVIEW STEP #5 – REVIEW DATA LOSS INDICATORS ON IDENTIFIED SYSTEMS

If the establishment of a backdoor, or other suspicious compromised behaviors are identified, it is then important to quantify what data has been accessed and what may have been exfiltrated.

Review all 'Data Loss Indicators' on the ALERT HEAT MAP, paying close attention to indicators related to 'Exfiltration over Alternate Protocols' (e.g., SCP / FTP) and other Internet-based transfers.



REVIEW STEP #6 – REVIEW ADDITIONAL 'DETECTION OPPORTUNITIES'

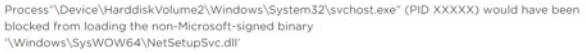
Several additional important detection opportunities have been provided by the FireEye Threat Research notification[2] as follows:

1. The malware utilized appears to be a "*memory only dropper that runs as a service, spawns a thread and reads from the file 'gracious_truth.jpg'*". Check for any instances of the creation of or access to this file in your environment:

   Source_File_Name:("gracious_truth.jpg")

   In addition, DTEX can be configured to log specific data inside Windows Event IDs. If this has been enabled in your environment, search for:

   EventLog_Event_ID:(12)

   
   Process "\Device\HarddiskVolume2\Windows\System32\svchost.exe" (PID XXXXX) would have been blocked from loading the non-Microsoft-signed binary '\Windows\SysWOW64\NetSetupSvc.dll'

2. "*The actor sets the hostnames on their command-and-control infrastructure to match a legitimate hostname found within the victim's environment. This allows the adversary to blend into the environment, avoid suspicion, and evade detection.*"

   Review any anomalous RDP access logs within DTEX. This can be done by creating a table to filter on the rare remote session activities to SolarWinds devices:

   Activity_Type:"SessionRemoteConnected"

3. "*The attacker's choice of IP addresses was also optimized to evade detection. The attacker primarily used only IP addresses originating from the same country as the victim, leveraging Virtual Private Servers.*"

   Review 'shared login' or 'impossible travel' of user accounts within the DTEX Platform. Please contact support@dtexsystems.com for access to advanced analytical methods to perform these checks.

4. "*Once the attacker gained access to the network with compromised credentials, they moved laterally using multiple different credentials. The credentials used for lateral movement were always different from those used for remote access.*"

   Review all DTEX Session Activity (Activity_Group:SessionActivity) and identify devices (Device_Name) with a one-to-many relationship between source systems and accounts.

5. "*The attacker used a temporary file replacement technique to remotely execute utilities: they replaced a legitimate utility with theirs, executed their payload, and then restored the legitimate original file. They similarly manipulated scheduled tasks by updating an existing legitimate task to execute their tools and then returning the scheduled task to its original configuration. They routinely removed their tools, including removing backdoors once legitimate remote access was achieved.*"

   Review the suspicious deleting of any executables that were created, executed and deleted within a short time frame (note that a 'correlation rule' can also be configured to identify this).

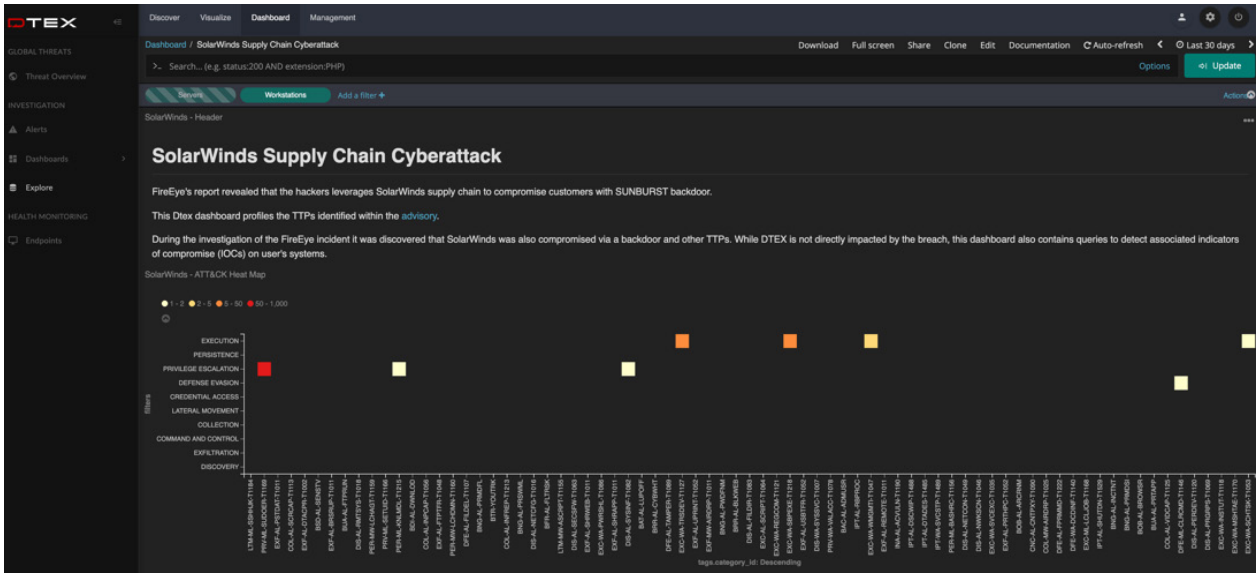
   Activity_Type:(FileDeleted OR FileCreated) AND Source_File_Extension:(exe)

2. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

REVIEW STEP #7 – INSTALL DTEX 'SOLARWINDS' THREAT ADVISORY DASHBOARD

As an additional review step, the DTEX Counter Insider Threat (C-InT) Team has created a real-time dashboard to help review unusual TTPs, in case they can be linked to the above-mentioned attack. This dashboard can be downloaded at the following link:
https://dtexsystems.freshdesk.com/a/solutions/articles/24000064277

The dashboard covers both DTEX's proprietary Insider Threat Kill Chain as well as the MITRE ATT&CK®[3] framework techniques highlighted in this advisory.



NEED FURTHER ASSISTANCE?

Please contact support@dtexsystems.com for further assistance from DTEX C-InT in any ongoing investigations or help in interpreting findings that may be related to this breach or any additional concerns related to Supply Chain Attacks.

The DTEX Counter Insider Threat (C-InT) has played a pivotal role in helping enterprise organizations identify and contextualize instances of account compromise, especially in instances where 'first-line-of-defense' cybersecurity controls have been ineffective. This has become particularly evident in sophisticated supply chain attacks where limited malware has been utilized, along with a high degree of stealth.

3. MITRE ATT&CK: https://attack.mitre.org/

DTEX CUSTOMER THREAT ADVISORY

SOLARWINDS SUPPLY CHAIN ATTACK