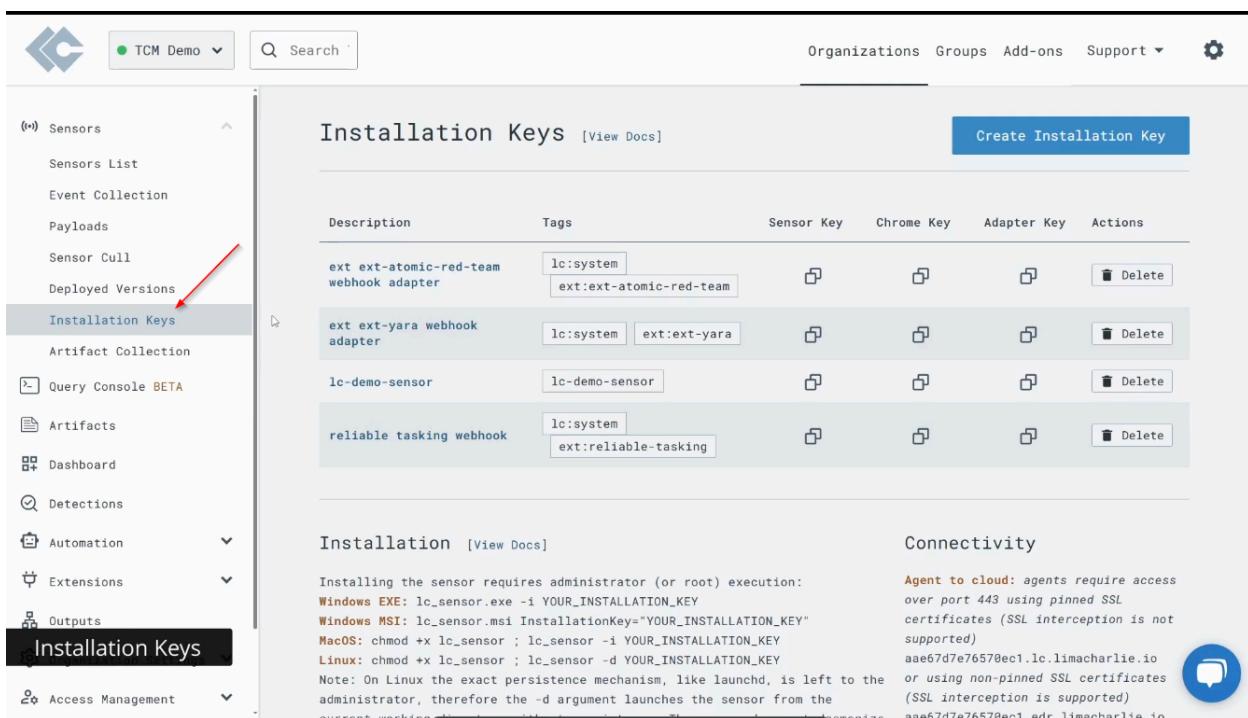


25. Lima Charlie - Deploying Endpoint Agents

Lima Charlie Install producer:

1.) Installation Keys



The screenshot shows the Lima Charlie Management interface. The left sidebar has a tree view with nodes like Sensors, Event Collection, Payloads, Sensor Cull, Deployed Versions, Installation Keys (which is highlighted with a red arrow), Artifact Collection, Query Console BETA, Artifacts, Dashboard, Detections, Automation, Extensions, Outputs, Access Management, and a bottom-level 'Installation Keys' node. The main content area is titled 'Installation Keys [View Docs]' and contains a table with four rows of data. The columns are Description, Tags, Sensor Key, Chrome Key, Adapter Key, and Actions. The data rows are:

Description	Tags	Sensor Key	Chrome Key	Adapter Key	Actions
ext ext-atomic-red-team webhook adapter	lc:system ext:ext-atomic-red-team	🔗	🔗	🔗	>Delete
ext ext-yara webhook adapter	lc:system ext:ext-yara	🔗	🔗	🔗	Delete
lc-demo-sensor	lc-demo-sensor	🔗	🔗	🔗	Delete
reliable tasking webhook	lc:system ext:reliable-tasking	🔗	🔗	🔗	Delete

Below the table, there are two sections: 'Installation [View Docs]' and 'Connectivity'. The Installation section provides instructions for different operating systems. The Connectivity section includes a note about agents requiring access over port 443 and a link to a support ticket.

TCM Demo ▾

Search

Organizations Groups Add-ons Support ▾

Sensors

- Sensors List
- Event Collection
- Payloads
- Sensor Cull
- Deployed Versions
- Installation Keys**
- Artifact Collection

Query Console BETA

Artifacts

Dashboard

Detections

Automation

Extensions

Outputs

Organization Settings

Access Management

Installation Keys [View Docs]

Create Installation Key

Description	Tags	Sensor Key	Chrome Key	Adapter Key	Actions
ext ext-atomic-red-team webhook adapter	lc:system ext:ext-atomic-red-team	<input type="button"/>	<input type="button"/>	<input type="button"/>	<input type="button"/> Delete
ext ext-yara webhook adapter	lc:system ext:ext-yara	<input type="button"/>	<input type="button"/>	<input type="button"/>	<input type="button"/> Delete
reliable tasking webhook	lc:system ext:reliable-tasking	<input type="button"/>	<input type="button"/>	<input type="button"/>	<input type="button"/> Delete

Installation [View Docs]

Installing the sensor requires administrator (or root) execution:

Windows EXE: lc_sensor.exe -i YOUR_INSTALLATION_KEY

Windows MSI: lc_sensor.msi InstallationKey="YOUR_INSTALLATION_KEY"

MacOS: chmod +x lc_sensor ; lc_sensor -i YOUR_INSTALLATION_KEY

Linux: chmod +x lc_sensor ; lc_sensor -d YOUR_INSTALLATION_KEY

Note: On Linux the exact persistence mechanism, like launchd, is left to the administrator, therefore the -d argument launches the sensor from the current working directory without persistence. The sensor does not daemonize itself.

Connectivity

Agent to cloud: agents require access over port 443 using pinned SSL certificates (SSL interception is not supported)

aae67d7e7e76570ec1.lc.limacharlie.io or using non-pinned SSL certificates (SSL interception is supported)

aae67d7e7e76570ec1.edr.limacharlie.io

Chrome Agent to cloud: agents require



Installation Keys [View Docs]

Create Installation Key

Description

Windows Lab Workstations

Tags (optional)

workstations, windows

Create

Installing the sensor requires administrator (or root) execution:
Windows EXE: lc_sensor.exe -i YOUR_INSTALLATION_KEY

Agent to cloud: agents re over port 443 using pinne

Sensors

- Sensors List
- Event Collection
- Payloads
- Sensor Cull
- Deployed Versions
- Installation Keys**
- Artifact Collection
- Query Console BETA
- Artifacts
- Dashboard
- Detections
- Automation
- Extensions
- Outputs
- Organization Settings
- Access Management

Installation Keys [View Docs]

Description	Tags	Sensor Key	Chrome Key	Adapter Key	Actions
Windows Lab Workstations	workstations windows				
ext ext-atomic-red-team webhook adapter	lc:system ext:ext-atomic-red-team				
ext ext-yara webhook adapter	lc:system ext:ext-yara				
reliable tasking webhook	lc:system ext:reliable-tasking				

Installation [View Docs]

Installing the sensor requires administrator (or root) execution:

```
Windows EXE: lc_sensor.exe -i YOUR_INSTALLATION_KEY
Windows MSI: lc_sensor.msi InstallationKey="YOUR_INSTALLATION_KEY"
MacOS: chmod +x lc_sensor ; lc_sensor -i YOUR_INSTALLATION_KEY
Linux: chmod +x lc_sensor ; lc_sensor -d YOUR_INSTALLATION_KEY
```

Note: On Linux the exact persistence mechanism, like launchd, is left to the administrator, therefore the -d argument launches the sensor from the

Connectivity

Agent to cloud: agents require access over port 443 using pinned SSL certificates (SSL interception is not supported)
aae67d7e76570ec1.lc.limacharlie.io or using non-pinned SSL certificates (SSL interception is supported)

This Sensor key very important so copy

Installation Keys [View Docs]

Description	Tags	Sensor Key	Chrome Key	Adapter Key	Actions
Windows Lab Workstations	workstations windows				
ext ext-atomic-red-team webhook adapter	lc:system ext:ext-atomic-red-team				
ext ext-yara webhook adapter	lc:system ext:ext-yara				
reliable tasking webhook	lc:system ext:reliable-tasking				

Download agent support OS case

But real case 10000 case endpoint there company so thus use ansible

The screenshot shows the Limacharlie web interface with the following details:

- Sensors** menu item is selected.
- Installation Keys** is highlighted in the sidebar.
- Sensor Downloads [View Docs]** section is displayed.
- EDR** tab is selected.
- Windows** section includes:
 - Windows 32 bit
 - Windows 64 bit (highlighted with a red arrow)
 - Windows ms132
 - Windows ms164
- macOS** section includes:
 - macOS 64 bit
 - macOS arm64
 - macOS package .pkg
- Linux** section includes:
 - Linux 32 bit
 - Linux 64 bit
 - Linux 32 bit .deb
 - Linux 64 bit .deb
 - Linux arm64
 - Linux arm64 bit .deb
 - Linux alpine64
 - Docker
- Chromium(/OS)** section includes:
 - Chrome
 - Edge
- Adapter** section includes:
 - Linux
 - Solaris
 - AIX
 - BSD
 - macOS
 - Windows
- Linux** section includes:
 - Linux 32 bit
 - Linux 64 bit
 - Linux arm
 - Linux arm64
- Solaris** section includes:
 - Solaris 64 bit
- AIX** section includes:
 - AIX ppc64
- BSD** section includes:
 - FreeBSD 64 bit
 - OpenBSD 64 bit
 - NetBSD 64 bit
- macOS** section includes:
 - macOS 64 bit
 - macOS arm64
- Windows** section includes:
 - Windows 64 bit

Install agent in machine:

Sensors are the primary input for data into LimaCharlie. They run on a variety of supported platforms and send JSON events to LimaCharlie's cloud in real-time. Embedded platforms (e.g. Windows, Mac, Linux) expose deeper capabilities like sending commands and collecting artifacts. Sensors tagged lc:system are generated by LimaCharlie Extensions and do not count towards the quota.

See active that windows host

Hostname	Tags	Last Seen/
desktop-c6oj5nl.net.rogers.com	windows workstations	2024-07-10 €
ext-atomic-red-team	ext:ext-atomic-red-team ... +1	2024-07-10 €
ext-yara	ext:ext-yara lc:system	2024-07-10 €
ext-reliable-tasking	ext:reliable-tasking lc:system	2024-07-10 €

Let analysis Features:

⇒ Note: EDR is solution but false positive always come so use manual skill analysis and always follow manual procedures

1.) Overview

The screenshot shows the Lima Charlie web interface. The top navigation bar includes a logo, a dropdown menu set to 'TCM Demo', a search bar, and links for 'Organizations', 'Groups', 'Add-ons', 'Support', and a gear icon. On the left, a sidebar menu lists various features: Analytics, Artifacts, Autoruns, **Console** (which is selected), Detections, Drivers, Event Collection, File System, Integrity Monitoring, Live Feed, Network, Packages, and Processes. The main content area displays 'Sensor Details' for the sensor 'desktop-c6oj5nl.net.rogers.com'. The sensor's status is shown as green with a checkmark. The details include:

Category	Value
Hostname	desktop-c6oj5nl.net.rogers.com
Platform	Windows x86 64 bit
Network Access	Allowed (Isolate From Network)
Kernel	Available
Seal Status	Not Sealed (Seal button)
Enrollment Date	2024-07-10 05:07:56
Last Time Alive	2024-07-10 05:08:02
Internal IP	192.168.1.9
External IP	08-00-27-BD-A6-EC
Mac Address	08-00-27-BD-A6-EC
Sensor ID	00b9df07-c52f-4140-a193-1405679ee5c9
Organization ID	1b6c5df7-ef3b-4521-bad6-f1f0ac9c13aa
Installer ID	Device ID

2.) Autoruns

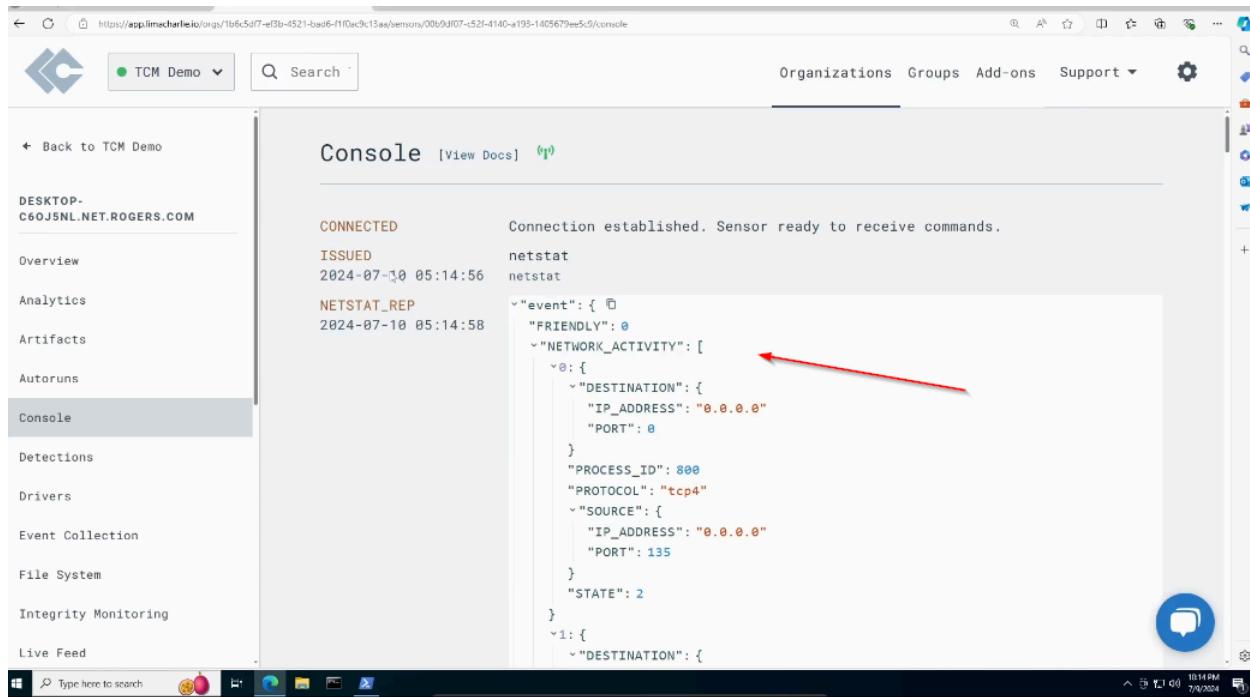
The screenshot shows the TCM Demo interface for the DESKTOP-C60J5NL.NET.ROGERS.COM sensor. The left sidebar has a red arrow pointing to the 'Autoruns' tab, which is highlighted in blue. The main content area is titled 'Autoruns [View Docs]' and displays a table of autorun entries:

Registry Key	Signed	File Path	Hash
SOFTWARE\Classes\Exefile\Shell\Open...	false	%1	
SOFTWARE\Classes\Exefile\Shell\Open...	false	%1	
SOFTWARE\Microsoft\Windows NT\Current...	false	explorer.exe	a7c7fd5f9cec332554ca7cdb
SOFTWARE\Microsoft\Windows NT\Current...	true	C:\Windows\system32\userinit.exe	0843369966e39c40b96c941e
SOFTWARE\Microsoft\Windows NT\Current...	true	SystemPropertiesPerformance.exe	b266318d45a4245556a2e39b
Software\Microsoft\Windows\CurrentV...	true	%windir%\system32\SecurityHealthSys...	ead5bbb7752377bb4d9bf8dc
Software\Microsoft\Windows\CurrentV...	true	%SystemRoot%\system32\VBoxTray.exe	1ef39a6ff5348a81078be56de
SYSTEM\CurrentControlSet\Control\Ls...	false	msv1_0	3c7466d9cf662d3dc6e6d230
SYSTEM\CurrentControlSet\Control\Ls...	false	scecli	7cf92060fabba8ac8e50c802

3.) Console

The screenshot shows the TCM Demo interface for the DESKTOP-C60J5NL.NET.ROGERS.COM sensor. The left sidebar has a red arrow pointing to the 'Console' tab, which is highlighted in blue. The main content area is titled 'Console [View Docs] ⓘ' and shows a status message: 'CONNECTED' and 'Connection established. Sensor ready to receive commands.' A red arrow points from the 'netstat' command input field at the bottom to the right.

Mini C2



The screenshot shows a web-based interface for monitoring endpoint activity. The left sidebar lists various monitoring categories: Overview, Analytics, Artifacts, Autoruns, Console (which is selected and highlighted in grey), Detections, Drivers, Event Collection, File System, Integrity Monitoring, and Live Feed. The main content area is titled "Console [View Docs]" and displays a log of network events. The log entries are:

- CONNECTED Connection established. Sensor ready to receive commands.
- ISSUED netstat 2024-07-10 05:14:56 netstat
- NETSTAT REP 2024-07-10 05:14:58 {"event": { "FRIENDLY": 0, "NETWORK_ACTIVITY": [{ "DESTINATION": { "IP_ADDRESS": "0.0.0.0", "PORT": 0 }, "PROCESS_ID": 800, "PROTOCOL": "tcp4", "SOURCE": { "IP_ADDRESS": "0.0.0.0", "PORT": 135 }, "STATE": 2 }, { "DESTINATION": { "IP_ADDRESS": "0.0.0.0", "PORT": 0 } }] }}

A red arrow points from the text "2024-07-10 05:14:58 {"event": {"FRIENDLY": 0, "NETWORK_ACTIVITY": ["0: {" to the word "0:" in the JSON log entry.

4.) File System:

File System

Name	Path	Size	Created
\$Recycle.Bin	c:\\$Recycle.Bin	-	2019-12-07 09:56:21
SWinREAgent	c:\\$WinREAgent	-	2024-07-09 21:00:00
Documents and Settings	c:\Documents and Settings	-	2024-05-13 18:00:00
PerfLogs	c:\PerfLogs	-	2019-12-07 09:56:21
Program Files	c:\Program Files	-	2019-12-07 09:56:21
Program Files (x86)	c:\Program Files (x86)	-	2019-12-07 09:56:21
ProgramData	c:\ProgramData	-	2019-12-07 09:56:21

5.) Network

Network

Local Port	Protocol	Foreign IP	Foreign Port	State	Process Hash
135	tcp4	0.0.0.0	0	LISTEN	6fc3bf1fdfd76860be782554f8d25bd32f108db934d70f4253f1e5f2352
139	tcp4	0.0.0.0	0	LISTEN	-
5840	tcp4	0.0.0.0	0	LISTEN	6fc3bf1fdfd76860be782554f8d25bd32f108db934d70f4253f1e5f2352
49664	tcp4	0.0.0.0	0	LISTEN	efa9e8325232bbd3f9a118d396de04370e56c3c7b6d552fab46b5b39f3a
49665	tcp4	0.0.0.0	0	LISTEN	21da0122ba7b723adad041969bded52eefaa99b47571670599bc03b3d7e1
49666	tcp4	0.0.0.0	0	LISTEN	6fc3bf1fdfd76860be782554f8d25bd32f108db934d70f4253f1e5f2352
49667	tcp4	0.0.0.0	0	LISTEN	6fc3bf1fdfd76860be782554f8d25bd32f108db934d70f4253f1e5f2352
49668	tcp4	0.0.0.0	0	LISTEN	abc2c4cd2a5de2fd6a2fb472b47517cfbcaee6138f4e52c68c042100db1
49707	tcp4	0.0.0.0	0	LISTEN	1efd9a81b2ddf21b3f327d67a6f8f88f814979e840885ec812af7a2180
49729	tcp4	13.107.246.254	443	CLOSE_WAIT	07a87f691372e5297fb7d2015f711dbda1d7a39263f5b53f2c8

6.) Process

The screenshot shows the TCM Demo application interface. On the left, a sidebar lists various monitoring categories: Autoruns, Console, Detections, Drivers, Event Collection, File System, Integrity Monitoring, Live Feed, Network, Packages, Processes (which is selected and highlighted with a red arrow), Services, and Timeline. Below the sidebar is a button labeled 'Processes'. The main content area is titled 'Processes (1)'. It features a 'Filter' input field containing 'i.e. 'evil.exe''. A second red arrow points to the 'Name' column header in a table below. The table has columns: Run, Name, PPID, PID, User, and Path. The data rows are:

Run	Name	PPID	PID	User	Path
⋮	System	0	4	NT AUTHORITY\SYSTEM	
⋮	Registry	4	72	NT AUTHORITY\SYSTEM	Regist...
⋮	smss.exe	4	320	NT AUTHORITY\SYSTEM	\Device\...
⋮	MemCompression	4	1652	NT AUTHORITY\SYSTEM	MemComp...
⋮	svchost.exe	580	352	NT AUTHORITY\LOCAL SERVICE	C:\Wind...
⋮	svchost.exe	580	368	DESKTOP-C60J5NL\tcm	C:\Wind...
⋮	svchost.exe	580	388	NT AUTHORITY\SYSTEM	C:\Wind...

7.) Services

TCM Demo Search Organizations Groups Add-ons Support

Autoruns
Console
Detections
Drivers
Event Collection
File System
Integrity Monitoring
Live Feed
Network
Packages
Processes
Services
Timeline
Services

Services [View Docs]

A list of services on this operating system.

SVC Name	SVC State	SVC Display Name	Executable	Hash
AarSvc_ba...	1	Agent Activation Runtime_ba530	C:\Windows\system32\svchost.exe -k _...	6fc3bf1fd76...
AJRouter	1	AllJoyn Router Service	%SystemRoot%\system32\svchost.exe -...	4e2623243a9bb...
ALG	1	Application Layer Gateway Ser...	%SystemRoot%\System32\alg.exe	3c3285b21d5c6...
AppIDSvc	1	Application Identity	%SystemRoot%\system32\svchost.exe -...	69e2d446d9849...
Appinfo	4	Application Information	%SystemRoot%\system32\svchost.exe -...	423d1bfb4f179...
AppMgmt	1	Application Management	%SystemRoot%\system32\svchost.exe -...	c3f02bb338eee...
AppReadin...	1	App Readiness	%SystemRoot%\System32\svchost.exe -...	1e0ed5eaf2dc8...
AppVClient	1	Microsoft App-V Client	%systemroot%\system32\AppVClient.exe	7a746e8d84e52...
AppXSvc	4	AppX Deployment Service (AppX_)	%systemroot%\system32\svchost.exe -...	6227e0375733f...

<https://app.limacharlie.io/orgs/1b6c5d7-e0b4-4521-bad6-f10ac9c15aa/sensors/00b9d07-c2f4-4142-a193-1405679ee5c9/services>

Services [View Docs]

Executable name:
C:\Windows\Sysmon64.exe

File Is Signed

Process Id
2668

Svc Display Name
Sysmon64

Svc Name
Sysmon64

Svc State
4

Svc Type
16

Hash
39b094613132377bc236f4ad940a3e02c544f86347c0179a9425edc1bd3b85cd

TapiSrv 1 Telephony %SystemRoot%\System32\svchost.exe -...

8.) Network Isolation

Network Isolation process

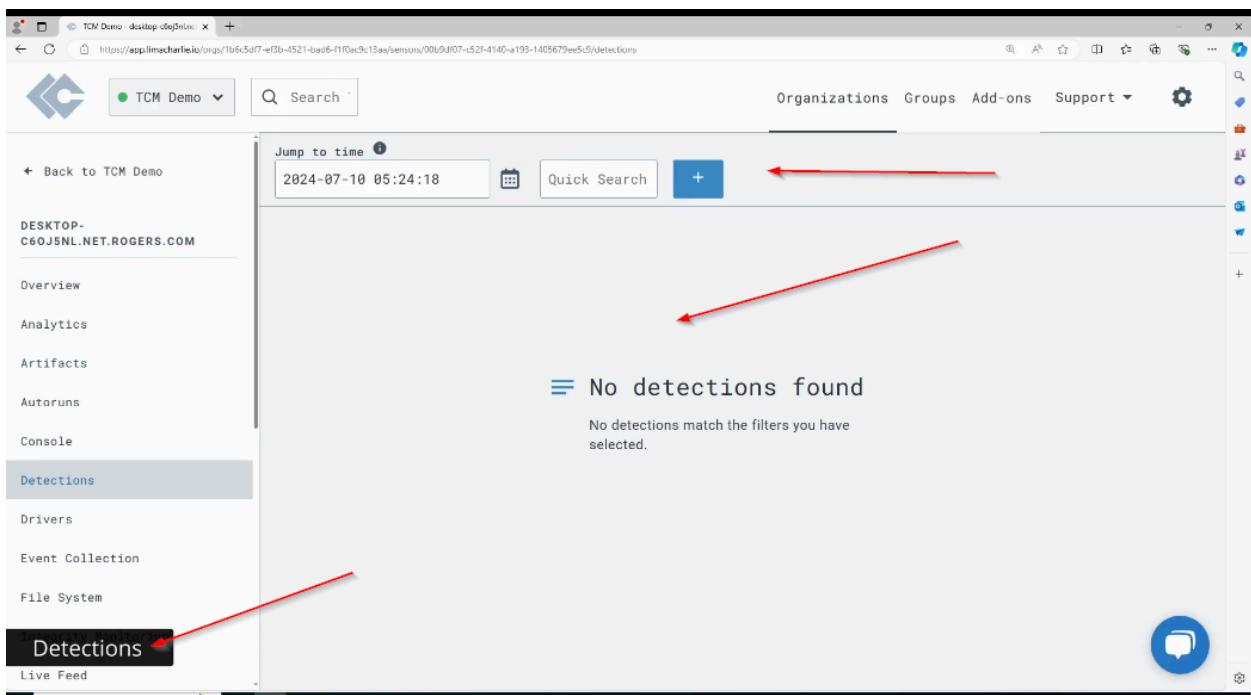
The screenshot shows the TCM Demo interface with the following details:

Sensor Details

Category	Value
Hostname	desktop-c6oj5nl.net.rogers.com
Platform	Windows x86 64 bit
Network Access	Allowed
Kernel	Available
Seal Status	Not Sealed
Enrollment Date	2024-07-10 05:07:56
Last Time Alive	2024-07-10 05:08:02
Internal IP	192.168.1.9
External IP	
Mac Address	08-00-27-BD-A6-EC
Sensor ID	00b9df07-c52f-4140-a193-1405679ee5c9
Organization ID	1b6c5df7-ef3b-4521-bad6-f1f0ac9c13aa
Installer ID	
Device ID	

A red arrow points to the "Isolate From Network" button under the Network Access section.

9.) Detections



Now Execute real malware (mimikatz tool) via use Lima charlie EDR:

⇒ Good EDR detection mimikatz tool execution

1.) First execute mimikatz

```
mimikatz 2.2.0 x64 (oe.eo)
06/27/2024 05:29 PM <DIR>      baseline
06/24/2024 02:36 PM <DIR>      exfil
07/09/2024 10:04 PM      780,080 hcp_win_x64_release_4.29.3.exe
07/08/2024 08:28 PM      1,250,056 mimikatz.exe
06/24/2024 02:20 PM      73,802 notmalware.exe
06/24/2024 04:29 PM <DIR>      ProcessExplorer
06/24/2024 04:28 PM      3,459,165 ProcessExplorer.zip
06/27/2024 06:49 PM <DIR>      Sysmon
06/27/2024 06:44 PM      4,858,922 Sysmon.zip
06/24/2024 02:55 PM <DIR>      TCPview
06/24/2024 02:54 PM      1,604,604 TCPView.zip
8 File(s)    15,124,914 bytes
8 Dir(s)   25,724,338,176 bytes free

C:\Users\tcm\Downloads>mimikatz.exe ←

.#####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # privilege::debug ←
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords ←
```

2.) See EDR detect malicious program

The screenshot shows the TCM Demo interface. The left sidebar has 'DESKTOP-C60J5NL.NET.ROGERS.COM' selected. The 'Detections' tab is highlighted. The main pane displays a 'Jump to time' bar set to '2024-07-10 05:32:46'. A red arrow points to the event list, which shows a single entry: '2024-07-10 05:27:07 HackTool - Mimikatz Execution desktop-c60j5nl.net.'. The right pane shows detailed information about this event, including its ID (f0f377ee-fab5-40ab-95e3-59f5668e1bab), category ('HackTool - Mimikatz Execution'), time ('2024-07-10 05:27:07'), source ('desktop-c60j5nl.net.rogers.com'), and a JSON log entry. Another red arrow points to the 'Source' field in the details pane.

The screenshot shows the TCM Demo interface. The left sidebar has 'DESKTOP-C60J5NL.NET.ROGERS.COM' selected. The 'Detections' tab is highlighted. The main pane displays a 'Jump to time' bar set to '2024-07-10 05:36:23'. A red arrow points to the event list, which shows three entries: '2024-07-10 05:32:28 00262-WIN-Suspicious_Lsass_Crossproc desktop-c60j5nl.net.rogers.com', '2024-07-10 05:32:00 HackTool - Mimikatz Execution desktop-c60j5nl.net.rogers.com', and '2024-07-10 05:27:07 HackTool - Mimikatz Execution desktop-c60j5nl.net.rogers.com'. The right pane shows a message 'You're up-to-date!' and a note 'That's all! No more past detections to fetch.'

```
    "detection": {  
        "author":  
            "_ext-sigma-7a14fbc3-54d9-4b4d-8700-61eddada  
            04f0[bulk][segment]"  
        "cat": "HackTool - Mimikatz Execution"  
        "detect": {  
            "event": {  
                "BASE_ADDRESS": 140695972675584  
                "COMMAND_LINE": "mimikatz.exe"  
                "FILE_IS_SIGNED": 1  
                "FILE_PATH":  
                    "C:\Users\tcm\Downloads\mimikatz.exe"  
                "HASH":  
                    "92804faaab2175dc501d73e814663058c78c0a0  
                    42675a8937266357bcfb96c50"  
                "MEMORY_USAGE": 9322496  
            }  
            "PARENT": {  
                "BASE_ADDRESS": 140699238662144  
                "COMMAND_LINE":  
                    "C:\Windows\system32\cmd.exe"  
                "FILE_IS_SIGNED": 1  
                "FILE_PATH":  
                    "C:\Windows\system32\cmd.exe"  
            }  
        }  
    }  
}
```

```
"detect_id":  
"f0f377ee-fab5-40ab-95e3-59f5668e1bab"  
"detect_mtd": {  
    "author":  
        "Teymur Kheirkhabarov, oscd.community, David ANDRE (additional keywords), Tim Shelton"  
    "description": "Detection well-known mimikatz command line arguments" ←  
    "falsepositives": [  
        0: "Unlikely"  
    ]  
    "level": "high"  
    "references": [ ←  
        0:  
            "https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment"  
        1:  
            "https://tools.thehacker.recipes/mz/modules"  
    ]  
}
```

4.) Then found malicious file check reputation to virustotal

We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).

File distributed by Benjamin Delpy

92804faaab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50
mimikatz.exe

Community Score: 61 / 71

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 16+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.mimikatz/marte Threat categories: trojan, hacktool, pua Family labels: mimikatz, marte, hacktools

Security vendors' analysis

AhnLab-V3	Trojan/Win32.RL_Mimikatz.R290617	Alibaba	Trojan:Win32/Mimikatz.4b2
AliCloud	HackTool:Win/Mimikatz.FZ	AIYac	Generic.Trojan.Mimikatz.Marte.lsl.A.CE9...
Anti-AVL	RiskWare/Win64.Mimikatz	Arcabit	Generic.Trojan.Mimikatz.Marte.lsl.A.CE9...
Avast	Win64.HacktoolX-gen [Tr]	AVG	Win64.HacktoolX-gen [Tr]
Avira (no cloud)	HEUR/ACEN.1364969	BitDefender	Generic.Trojan.Mimikatz.Marte.lsl.A.CE9...

Type here to search

4.) Process analysis

TCM Demo

Search

Organizations Groups Add-ons Support

Detections Drivers Event Collection File System Integrity Monitoring Live Feed Network Packages Processes Services Timeline Users

Hostname: desktop-c60j5nl.net.rogers.ca

Processes

Filter: mimika

Run	Name	PPID	PID	User	Path
	mimikatz.exe	1948	6840	DESKTOP-C60J5NL\tcm	C:\User