Attack technique report

Demo

Credential Dump

Technique description

An attacker can dump your credentials for later reuse if you log in to a machine using Interactive Logon.

MITRE technique alignment

T1003 ,T1003.001 ,T1003.002 ,T1003.003 ,T1003.004

Interactive logon provides attackers with an opportunity to dump your credentials for later reuse.

Typically, the attacker performs Credential Dump on credentials you enter from a local keyboard, but RDP also provides an additional opportunity. Third-party tools like Psexec enable remote interactive logon.

About EDR solutions against credential dumping

People use EDR (Endpoint detection and response) solutions to protect your endpoints from Credential Dump. However, EDR is not enough to prevent Credential Dump. Attackers know ways to bypass the EDR protection techniques easily. They can bypass the EDR to perform Credential Dump from the kernel or from user mode, and also to perform Token Manipulation. See the Help Desk article EDR Bypass for more information about the ways attackers bypass the EDR.

Reference

- Interactive logon
- RDP
- Psexec
- EDR Bypass

Remediations

- When using RDP restrictedAdmin, connect with untrusted machines only from trusted machines
- Use Microsoft Windows Defender Credential Guard when possible
- Use Microsoft Protected Process Light to protect critical processes
- Add privileged domain accounts to the Protected Users group
- Do not use interactive logon to manage computers

When using RDP restrictedAdmin, connect with untrusted machines only from trusted machines

Remediation (1 of 5)

RDP Restricted Admin

Restricted Admin Mode is feature of RDP allowing users to login without leaving their passwords on the target machine they are connecting to.

Restricted Admin is good for Help Desk activities since is supports interactive connection to various machines without risk of leaving broad credentials on those machines.

Restricted Admin can also expose organizations to Pass The Hash exploits, making it most useful as a last resort or used when Pass-the-Hash attacks are mitigated through other means.

Enable Restricted Admin

To enable restricted admin read this.

Use Microsoft Windows Defender Credential Guard when possible

Remediation (2 of 5)

Credential Guard

The Credential Guard feature in Windows 10 employs a Virtual Machine to protect credentials from dumping tools like Mimikatz.
Credential Guard is a more robust solution, unlike Microsoft Protected Process Light, which is easily bypassed.

Unfortunately, attackers can also bypass Credential Guard using Access Tokens. Regardless, Credential Guard is probably the best passive protection currently available.

Enabling Credential Guard

Configuration of Credential Guard may also involve modification of BIOS settings, requiring local access to the machine (not remote). Learn more about the process at Credential Guard Management.

Credential Guard Requirements

- Windows Defender Credential Guard: Requirements

Use Microsoft Protected Process Light to protect critical processes

Remediation (3 of 5)

Protected Process Light

PPL provides protection around the LSASS process, limiting the ability of attackers to dump memory and steal passwords.

While Protected Process Light can be bypassed with tools like Mimikatz signed driver, it's still a recommended solution to protect in-memory passwords from low-skill bad actors.

...

Add privileged domain accounts to the Protected Users group

Remediation (4 of 5)

Protected Users

Microsoft Protected Users Group is an Active Directory group in which every user is restricted to using Kerberos tickets for authentication. Since Kerberos tickets expire in a relatively short time and are not renewable, they provide greater protection from credential theft and abuse.

Limitations of using the Protected User Group

Users in the group still use TGT that are subject to attacks like Pass-the-ticket.

The XM Cyber tools will still attack those Ticket-Granting Tickets (TGTs) to steal domain credentials.

Do not use interactive logon to manage computers

Remediation (5 of 5)

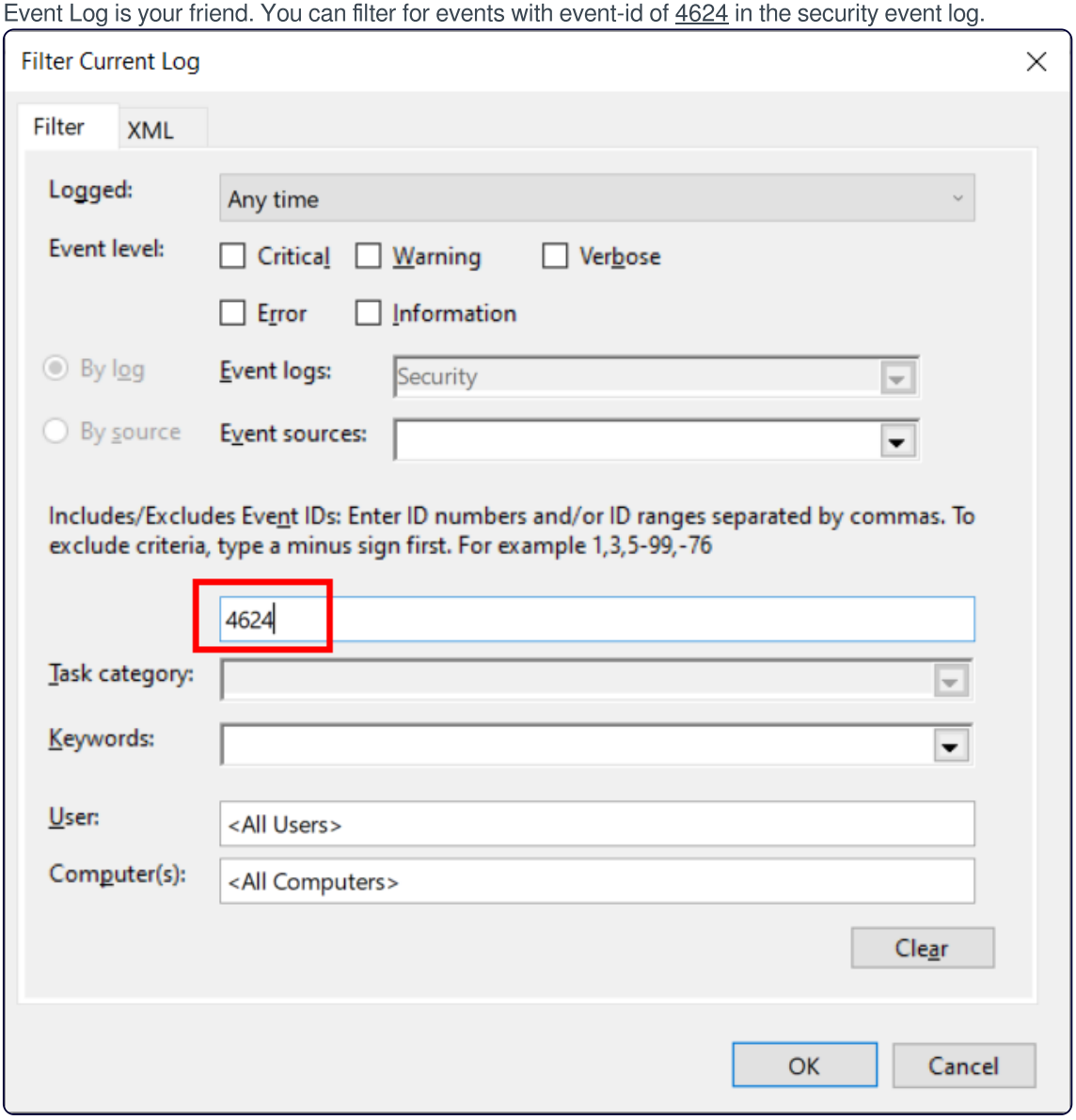
How can attackers dump/grab credentials?

Credential grabbing is most often the result of what Microsoft terms Interactive Logons. Prototypically, interactive logon (and associated credential grabbing) occurs at a local keyboard, but RDP provides equal opportunity for credential grabbing. In fact, third party tools like Psexec also enable remote interactive login.

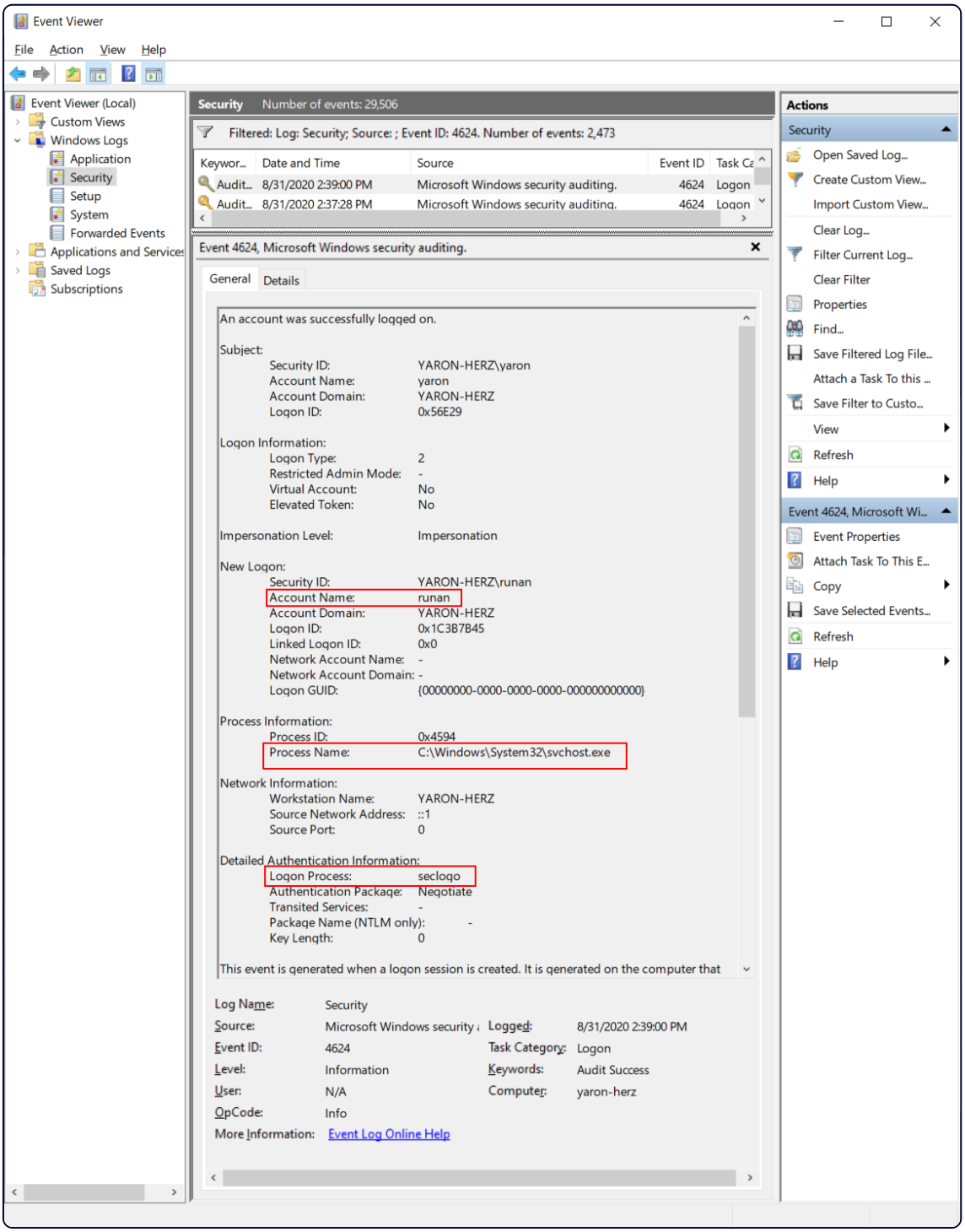
When users log in interactively, they must supply their credentials (username and password), providing attackers with an immediate opportunity to steal and re-use those credentials.

How to track interactive logon activity

Event Log is your friend. You can filter for events with event-id of 4624 in the security event log.



From the filtered list, you can determine which users are connected via interactive login or have connected that way in the past.



Entries tagged as Logon Type 2 indicate an interactive logon - see event description.

To run equivalent queries on the Event Log from the command line, enter the following:

```
WEVTUtil query-events /count:1000 Security /rd:true /format:text "/q:*[System
[(EventID=4624)]] and *[EventData[Data[@Name='TargetUserName']='<SOME_USER>']]"
```

Login events from the Security Event Log can indicate the origin of an interactive login, and often also the the IP address of the computer that performed the authentication and the ID of the process involved.

Safer logon events

The interactive logon method is not a must in all cases. Many times interactive logon is used to manage other computers. There are better approaches to manage remote machines without leaving credentials behind, by using Microsoft Restricted Admin or other Network Logon methods. Find additional information regarding exposing credentials via remote logon in this Microsoft article.