Mimikatz Update Fixes Forged Kerberos Ticket Domain Field Anomaly – Golden Ticket Invalid Domain Field Event Detection No Longer Works

adsecurity.org

Sean Metcalf January 5, 2016

In late 2014, I discovered that the domain field in many events in the Windows security event log are not properly populated when forged Kerberos tickets are used. The key indicator is that the domain field is blank or contains the FQDN instead of the short (netbios) name and depending on the tool used to generate the Kerberos tickets, other domain field anomalies may be present in the events.
The likely reason for the anomalies is that third party tools that create Kerberos tickets (TGT & TGS) don't format the tickets exactly the same way as Windows does.

Around this time last year (early January 2015), I shared with customers these indicators for detecting forged Kerberos tickets and subsequently presented this information at BSides Charm 2015. Soon after, Mimikatz was updated with a domain field that was set to static values, usually containing the string "eo.oe".

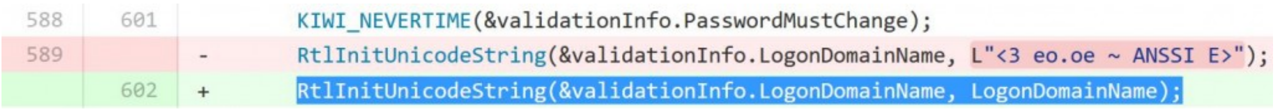
As of 4/16/2015: Mimikatz generated tickets may include the string "eo.oe.kiwi :) " in the domain field.
As of 6/29/2015: Mimikatz generated tickets may include the string "<3 eo.oe – ANSSI E>" in the domain field.

Few things in life are as consistent as the guarantee that things will change. In infosec, that means the attack tools will continue to evolve to evade detection and the defensive tools need to constantly evolve and improve.

If you protect your Active Directory admins (and service accounts), you will likely not have to deal with forged Kerberos Tickets since they require prior admin access. The problem is that Active Directory & Enterprises are often not secured to protect against modern threats and often, gaining Domain Admin rights to an AD domain is often too easy in many enterprises.

Detecting forged Kerberos tickets, including Golden Tickets and Silver Tickets, by identifying for domain field anomalies is likely no longer possible. As of the Mimikatz update dated 1/5/2016, forged Kerberos tickets no longer include a domain anomaly since the netbios domain name is placed in the domain component of the Kerberos ticket.

Mimikatz code diff:



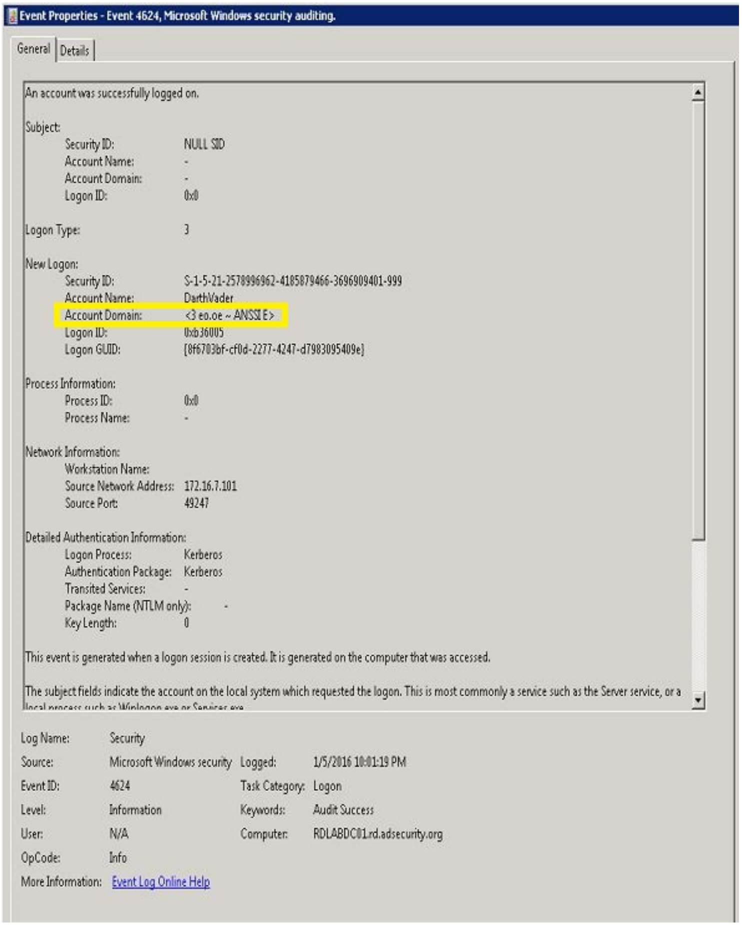
```
      KIWI_NEVERTIME(&validationInfo.PasswordMustChange);
-     RtlInitUnicodeString(&validationInfo.LogonDomainName, L"<3 eo.oe ~ ANSSI E>");
+     RtlInitUnicodeString(&validationInfo.LogonDomainName, LogonDomainName);
```

This means that attackers using the Mimikatz version dated 1/5/2016 and/or Invoke-Mimikatz with this updated DLL will likely not trigger alerts based on the invalid domain fields I identified in the past.

User behavior analysis tools such as Microsoft Advanced Threat Analytics (ATA) is the best current method to detect this and other attack types. The best way to detect Golden Tickets is to correlate TGS requests to prior TGT requests. If there's no prior TGT request (within a threshold), then the TGS request may be related to a Golden Ticket.

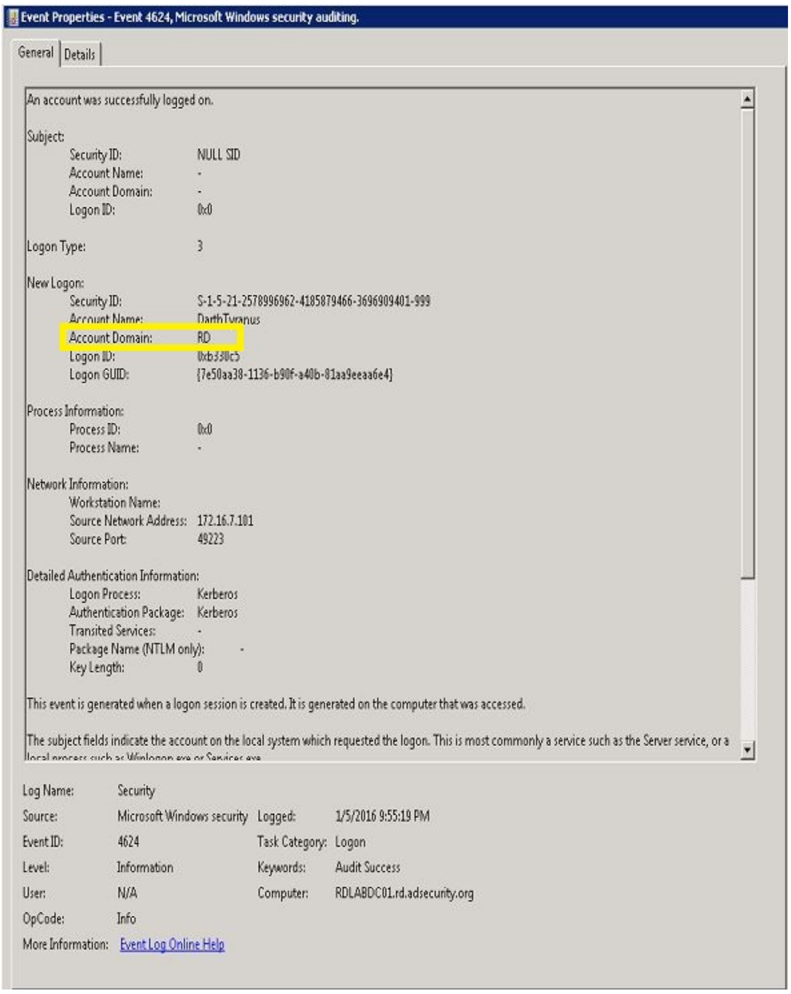
Golden Ticket event from using Mimikatz dated (11/2015): Has the an invalid domain value ("*<3 eo.oe – ANSSI E>*")

Golden Ticket event from using Mimikatz dated (1//05/2015): Has the correct domain value ("RD")


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details

```
An account was successfully logged on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

New Logon:
        Security ID:            S-1-5-21-2578996962-4185879466-3696909401-999
        Account Name:           DarthVader
        Account Domain:         <3 eo.oe ~ ANSSI E>
        Logon ID:               0xb36005
        Logon GUID:             {8f6703bf-cf0d-2277-4247-d7983095409e}

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:
        Source Network Address: 172.16.7.101
        Source Port:            49247

Detailed Authentication Information:
        Logon Process:          Kerberos
        Authentication Package: Kerberos
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a
local process such as Winlogon.exe or Services.exe
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:         1/5/2016 10:01:19 PM
Event ID:          4624                         Task Category:  Logon
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       RDLABDC01.rd.adsecurity.org
OpCode:            Info
More Information:  Event Log Online Help
```


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details

```
An account was successfully logged on.

Subject:
        Security ID:              NULL SID
        Account Name:             -
        Account Domain:           -
        Logon ID:                 0x0

Logon Type:                       3

New Logon:
        Security ID:              S-1-5-21-2578996962-4185879466-3696909401-999
        Account Name:             DarthTyranus
        Account Domain:           RD
        Logon ID:                 0xb330c5
        Logon GUID:               {7e50aa38-1136-b90f-a40b-81aa9eeaa6e4}

Process Information:
        Process ID:               0x0
        Process Name:             -

Network Information:
        Workstation Name:
        Source Network Address:   172.16.7.101
        Source Port:              49223

Detailed Authentication Information:
        Logon Process:            Kerberos
        Authentication Package:   Kerberos
        Transited Services:       -
        Package Name (NTLM only):        -
        Key Length:               0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a
local process such as Winlogon.exe or Services.exe.
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:         1/5/2016 9:55:19 PM
Event ID:          4624                         Task Category:  Logon
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       RDLABDC01.rd.adsecurity.org
OpCode:            Info
More Information:  Event Log Online Help
```

I have updated the appropriate references:

(Visited 6,118 times, 1 visits today)