What's New in the Windows 10 Security Log

JANUARY 2016

A Randy Franklin Smith white paper commissioned by LogRhythm Inc

Among the countless changes in Windows 10 Microsoft has provided IT organizations more visibility into auditable actions on Windows 10 machines and the resulting events in the Security Log. Understanding these enhancements is important because we need every edge we can get to detect endpoint intrusions.

Threat actors use a sophisticated mix of phishing, social engineering, and malware to attempt to compromise any user within an organization. A seemingly benign order request sent to a salesperson or a benefits summary to someone in HR can contain attachments infected with malware. Once such payloads are in, the goal is to determine how to leverage current users and other accounts on the compromised machine to access valuable and sensitive data, as well as how to spread out within the organization and repeat the process.

To help in thwarting these actions, Microsoft has added specific auditing and logging events in an effort to empower IT organizations to determine when potential threat actions are being performed:

- **Scoping user privileges.** To determine the value of the user accounts on the compromised machine, threat actors begin by scoping out local credentials and investigating which privileges the current user and other user accounts on the local machine have. Group memberships are enumerated for each local account to identify group affiliations that might provide additional access to systems, applications, or data.
- **Logging on with additional credentials.** Should threat actors find an account such as a local Admin with no password, they can use such accounts to gain further access to local and remote data and resources.
- **Launching hacking tools.** After compromising the machine, threat actors begin to take advantage of any and all tools—be it a simple command line, use of PowerShell, or an externally obtained executable—to expand their breadth of access to systems, applications, and data within your network.
- **Connecting to other machines.** To maximize their chances of success in finding, obtaining, and extracting valuable data, threat actors seek to connect to as many machines as possible.

In this white paper, we'll look at new and updated event entries in Windows 10, educating you on specific changes, what new detail is provided, and how to leverage these new events to identify malicious activity.

Turning Data into Insight: The LogRhythm Labs' Machine Data Intelligence Group

Vendors such as Microsoft realize that IT organizations need critical audit events as potential security threats occur. But on their own, events represent only data. Without additional facts, that information can easily be misunderstood, as well as lost in a sea of other events. What IT organizations really need is the intelligence that results from consuming and correlating the vast number of events across a multitude of operating systems and hardware, providing IT with actionable insight.

Organizations immediately look to SIEM and log management solutions to provide that intelligence. But while SIEM products have generally been effective at collecting audit logs and running user-supplied queries, their promise to make the leap on their own from raw data to actionable intelligence has frequently fallen short.

That's what makes LogRhythm's approach different. The Machine Data Intelligence (MDI) group in LogRhythm Labs is committed to building intelligence into LogRhythm for every significant log source and keeping it up to date. This examination of new security events in the Windows Security Log is a great example of their follow through on this commitment.

The Machine Data Intelligence (MDI) group in LogRhythm Labs does more than just document new events. It has taken on the challenge of turning raw data into insight, providing visibility into events across a long list of hardware and software sources, including Windows 10. With each new or changed event, the data is parsed, generating a new or updated regular expression that can be mapped to an already extensive common event model. In this model, events and their data are classified within an event taxonomy, allowing similar events from disparate systems to be automatically leveraged against existing correlation rules, as well as creating new opportunities to detect suspicious activity.

This tremendous investment—which LogRhythm calls knowledge engineering—enables easy identification, trending, and analysis of events across an entire IT environment, empowering automated incident response.

By making the investment in knowledge engineering, LogRhythm continually builds momentum on its normalized architecture, which appreciates in value with each new operating system, network device, and log data source.

Look for insights from the LogRhythm Labs' MDI group on how to leverage these new Windows Security Log events for enhanced threat detection throughout this paper.

Scoping User Privileges

After a system is compromised, the first action of a threat actor is to assess the current state of access by determining whether the breached user is privileged and if it is not, they will search for other accounts with higher privileges on the compromised machine. This kind of information potentially allows the threat actor to target those users via pass-the-hash attacks.

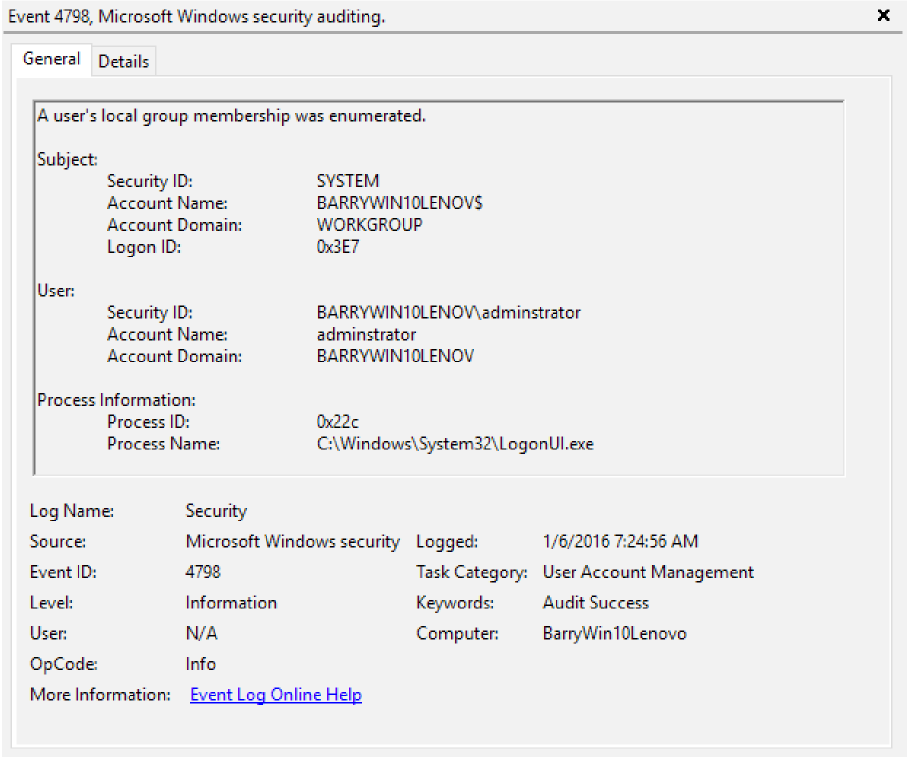
Event 4798: To Which Groups Does This User Belong?

When a user's local group memberships are enumerated, Windows 10 now generates event ID 4798, as shown in the following figure. This event documents the enumeration, which user was enumerated, the user who requested the enumeration, and which process was used to perform the enumeration.

Seeing an enumeration performed by any account other than the domain admin (which might be modifying local memberships) or via any process other than MMC.exe (such as via a NET LOCAL command) might indicate inappropriate activity. These details can help a Security Information and Event Management (SIEM) solution properly filter out approved activity.

To generate this detailed event, you need to enable the ***Audit User Account Management*** policy. You should enable this policy on all endpoints, including domain controllers.

On domain controllers, this audit policy tracks the enumeration of domain user accounts, whereas member servers and Windows 10 clients track the enumeration of local user accounts.



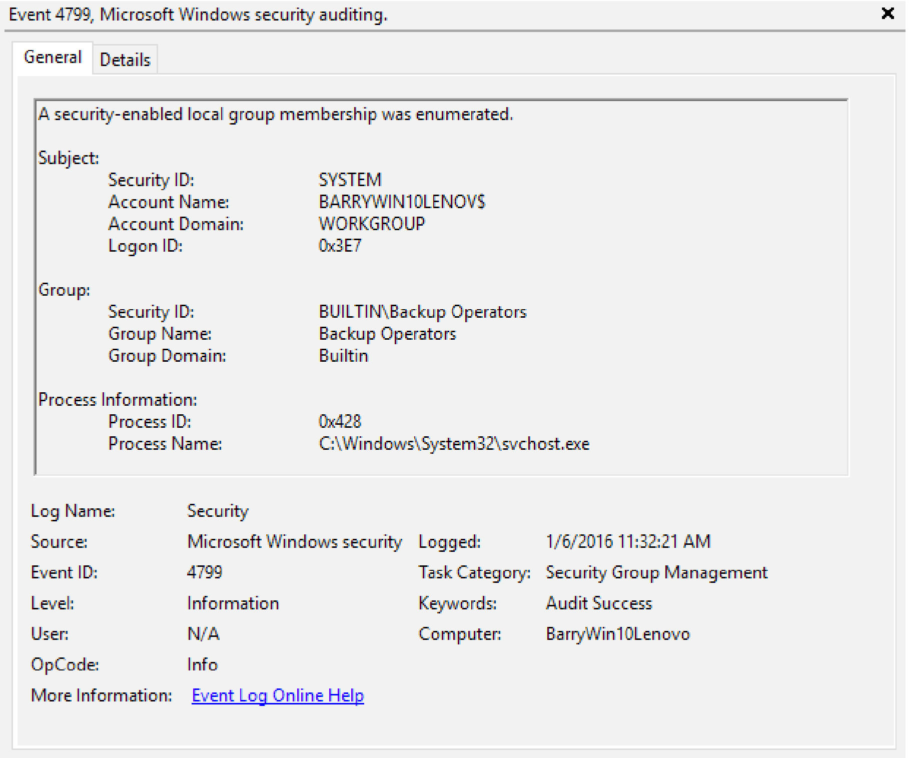
```
A user's local group membership was enumerated.

Subject:
        Security ID:            SYSTEM
        Account Name:           BARRYWIN10LENOV$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

User:
        Security ID:            BARRYWIN10LENOV\adminstrator
        Account Name:           adminstrator
        Account Domain:         BARRYWIN10LENOV

Process Information:
        Process ID:             0x22c
        Process Name:           C:\Windows\System32\LogonUI.exe
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          1/6/2016 7:24:56 AM
Event ID:          4798                          Task Category:   User Account Management
Level:             Information                   Keywords:        Audit Success
User:              N/A                           Computer:        BarryWin10Lenovo
OpCode:            Info
More Information:  Event Log Online Help
```

Event 4799: Who Are Members of This Local Group?

In another spin on the same attack vector, a threat actor starts with a known local group (such as the local Administrators group) and works to figure out who is in that group by enumerating its members (instead of starting with a user and enumerating the groups to which that user belongs).

When local groups are enumerated, Windows 10 can be configured to generate event 4799, which documents the enumerated group, the user that requested the enumeration, and the process name that was used to perform the enumeration. This event requires you to enable generation of the ***Audit Security Group Management*** policy.



```
A security-enabled local group membership was enumerated.

Subject:
        Security ID:            SYSTEM
        Account Name:           BARRYWIN10LENOV$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Group:
        Security ID:            BUILTIN\Backup Operators
        Group Name:             Backup Operators
        Group Domain:           Builtin

Process Information:
        Process ID:             0x428
        Process Name:           C:\Windows\System32\svchost.exe
```

```
Log Name:         Security
Source:           Microsoft Windows security   Logged:         1/6/2016 11:32:21 AM
Event ID:         4799                         Task Category:  Security Group Management
Level:            Information                  Keywords:       Audit Success
User:             N/A                          Computer:       BarryWin10Lenovo
OpCode:           Info
More Information: Event Log Online Help
```

LogRhythm MDI Insight

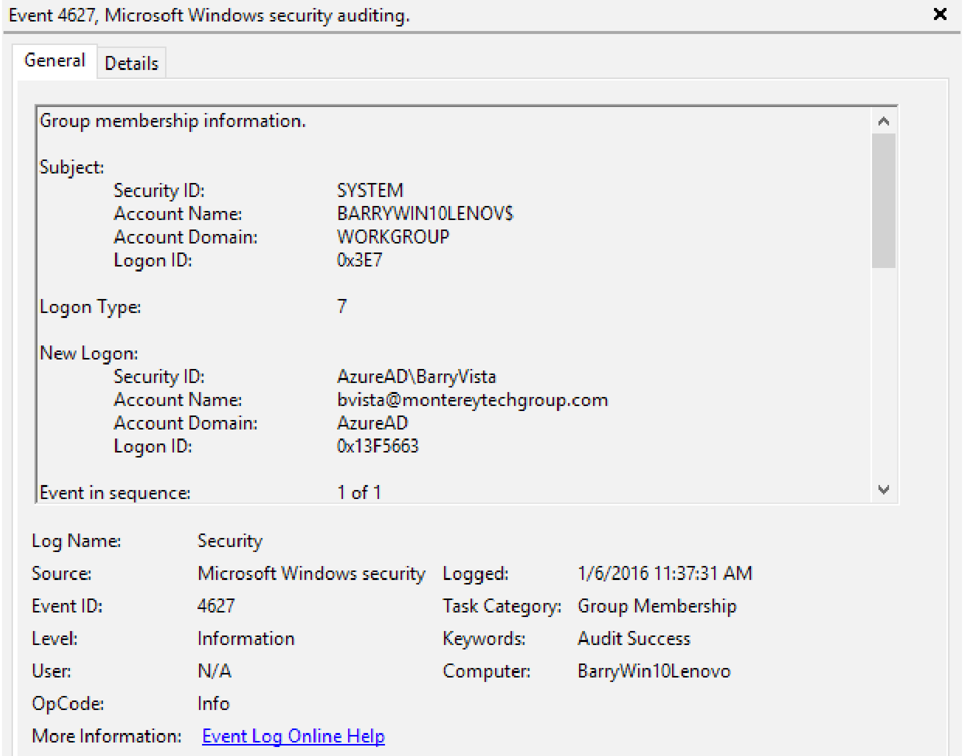
Using dynamic baselining, focus on the responsible process—typically Microsoft Management Console (MMC). Use trending to identify what is "normal" in your environment and to notify you when a new process is responsible for causing this event. Even if the appropriate process changes in the next version of Windows, the beauty of dynamic baselining is that IT gets a notification the first time the responsible process changes, at which time IT can determine whether action is required. That new process then becomes part of the baseline, eliminating multiple false positives.

User's Group Membership Documented at Logon

When you enable the Audit Logon policy to identify when users log on to a system, a new Audit Group Membership policy is added under the Logon/Logoff category. Enabling this policy generates the 4627 event at logon or any time a new account is used to launch a new process or new session.

Whereas event 4688 shows the launch of a new process and the credentials that are used, event 4627, which is shown in this figure, augments event 4688 by detailing the group memberships of the logged-on user.

Note that both local and domain group memberships for the logged-on user are detailed. More than one event may be logged for a single logon when the enumeration of groups requires more space than a single event entry can hold. (The event in sequence value shows both the total number of events in this enumeration and the position of the given event within that sequence.)


Event 4627, Microsoft Windows security auditing.

```
Group membership information.

Subject:
        Security ID:            SYSTEM
        Account Name:           BARRYWIN10LENOV$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Type:                     7

New Logon:
        Security ID:            AzureAD\BarryVista
        Account Name:           bvista@montereytechgroup.com
        Account Domain:         AzureAD
        Logon ID:               0x13F5663

Event in sequence:              1 of 1
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/6/2016 11:37:31 AM
Event ID:	4627	Task Category:	Group Membership
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	BarryWin10Lenovo
OpCode:	Info		
More Information:	Event Log Online Help		

LogRhythm MDI Insight

This event can be leveraged when you are interested in knowing whether a user of a certain authority (as defined by group membership) has been used. Analysing this membership list enables the direct real-time monitoring of accounts with elevated privileges, where an unusual pattern can trigger an alert.

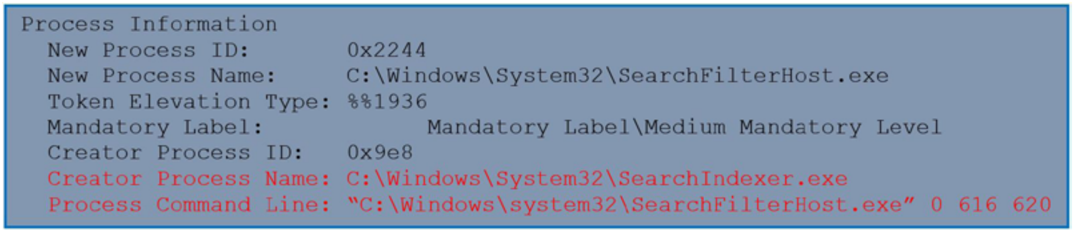
Launching Hacking Tools

Threat actors will use any tools and utilities at their disposal. One of the ways that Microsoft has worked to keep IT informed is via event 4688, which documents when a new process has been created. With Windows 10, this event is improved to provide more context around new processes.

More Detail on EXE Process Execution in Windows 10

In recent years it's become more important not only to know what process was started but what process started that process (AKA the parent or creator process). Earlier versions of event 4688 simply provided the process ID of the parent process, requiring you to research and cross-reference events to identify which the actual executable name that ID equated to. With Windows 10, the full path of the creator process name is clearly labeled.

Some executables are rather generic and started frequently for many different purposes. The secret to why the process was started and what it did is often in the command line passed to the process. This data was missing in 4688 in past versions, but Windows 10 brings a new and significant field to the 4688 event: Process Command Line, shown in red in the following figure. This allows you to capture not just the name of the EXE but the full command line that was used, showing the path, parameters, arguments, and switches of the command and providing visibility into its intent and purpose.



```
Process Information
  New Process ID:        0x2244
  New Process Name:      C:\Windows\System32\SearchFilterHost.exe
  Token Elevation Type:  %%1936
  Mandatory Label:             Mandatory Label\Medium Mandatory Level
  Creator Process ID:    0x9e8
  Creator Process Name:  C:\Windows\System32\SearchIndexer.exe
  Process Command Line:  "C:\Windows\system32\SearchFilterHost.exe" 0 616 620
```

This added detail is not logged by default. To get it, you need to enable the ***Include command line in process creation events*** policy under the Audit Process Creation administrative template.

LogRhythm MDI Insight

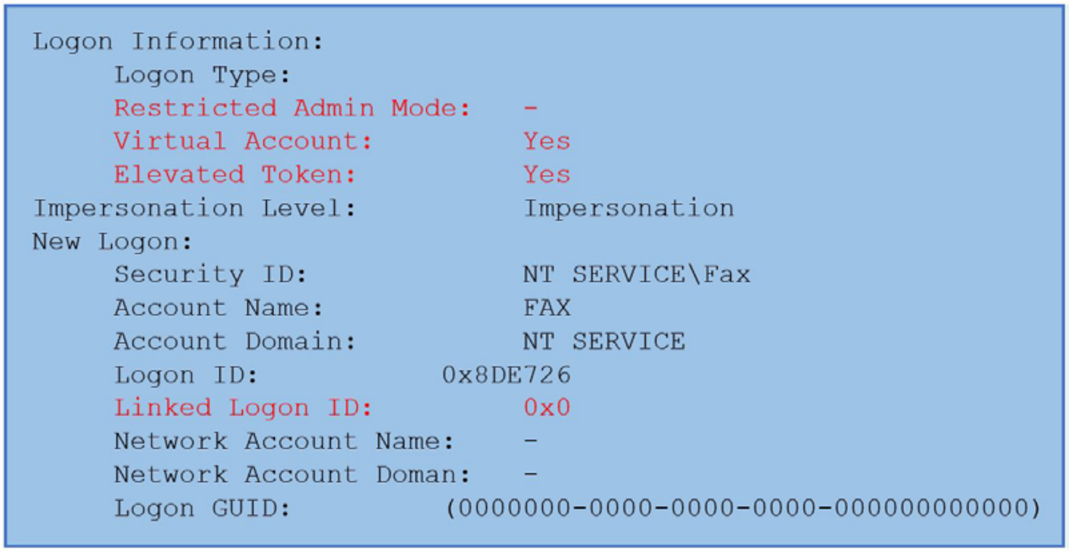
The command-line detail can be used to document more than command switches; command-line parameters can contain user accounts and passwords so be aware that enabling this option can cause such credentials to be captured in the Security Log. But the great value of this event detail is that it can also be used to track malware that perpetuates itself by spawning another process, changing the process name each time.

Connecting to Machines

No threat actor is satisfied with simply compromising a single machine within an organization; the goal is to seek out and compromise as many other systems as possible, each one potentially providing access to valuable data. Event 4264 is logged whenever a logon occurs in any way, shape, or form: interactively on the local console, remotely via remote desktop, by connecting via a shared folder or other network resource, by starting a service, and so on.

Changes to Logon Event 4624

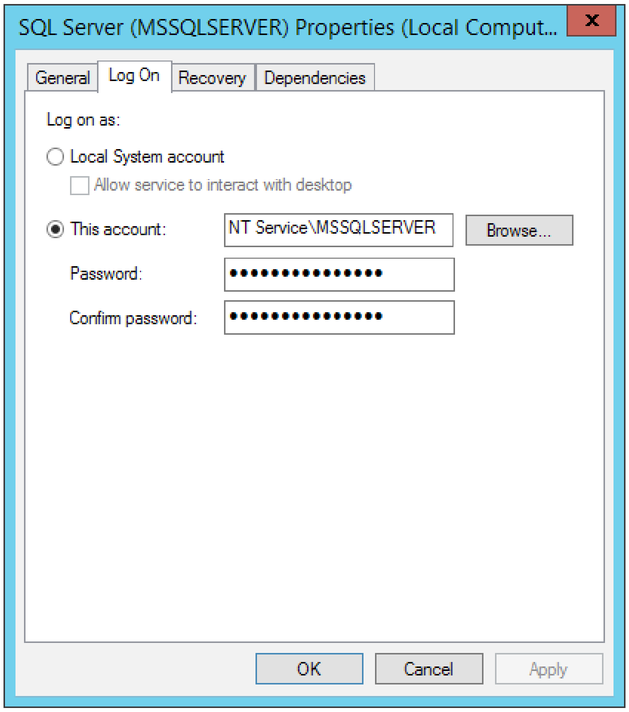
Windows 10 enhances this event by incorporating several new fields (shown in red in the following figure), providing additional context around various types of logons.



```
Logon Information:
     Logon Type:
     Restricted Admin Mode:   -
     Virtual Account:         Yes
     Elevated Token:          Yes
Impersonation Level:          Impersonation
New Logon:
     Security ID:             NT SERVICE\Fax
     Account Name:            FAX
     Account Domain:          NT SERVICE
     Logon ID:           0x8DE726
     Linked Logon ID:         0x0
     Network Account Name:    -
     Network Account Doman:   -
     Logon GUID:         (0000000-0000-0000-0000-000000000000)
```

The following fields have been added to event 4624:

- **Restricted Admin Mode.** This field applies only to remote desktop logons to protect credentials against “pass-the-hash” attacks. If enabled, this event reflects a logon type of 10 in addition to denoting Yes next to this field.
- **Virtual Account.** A virtual account is one that you create under the Log On properties of a service, as shown in this figure. Trying to audit what local services are doing is difficult when they all show up as running as LocalSystem or Network Service, leaving you unsure which service is responsible for the logon. By providing a fictitious account name that must match the service name (preceded by NT SERVICE\), that account name is populated in the Virtual Account field, allowing IT to match a logon with a service.
- **Elevated Token.** Related to User Account Control (UAC), this field populates with a Yes when you use an elevated account to launch a session or process.
- **Linked Logon ID.** This field is filled in only during session unlocks or during logons with cached credentials. The ID value links back to the originating session ID.



SQL Server (MSSQLSERVER) Properties (Local Comput...

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: NT Service\MSSQLSERVER

Password: •••••••••••••••

Confirm password: •••••••••••••••

LogRhythm MDI Insight

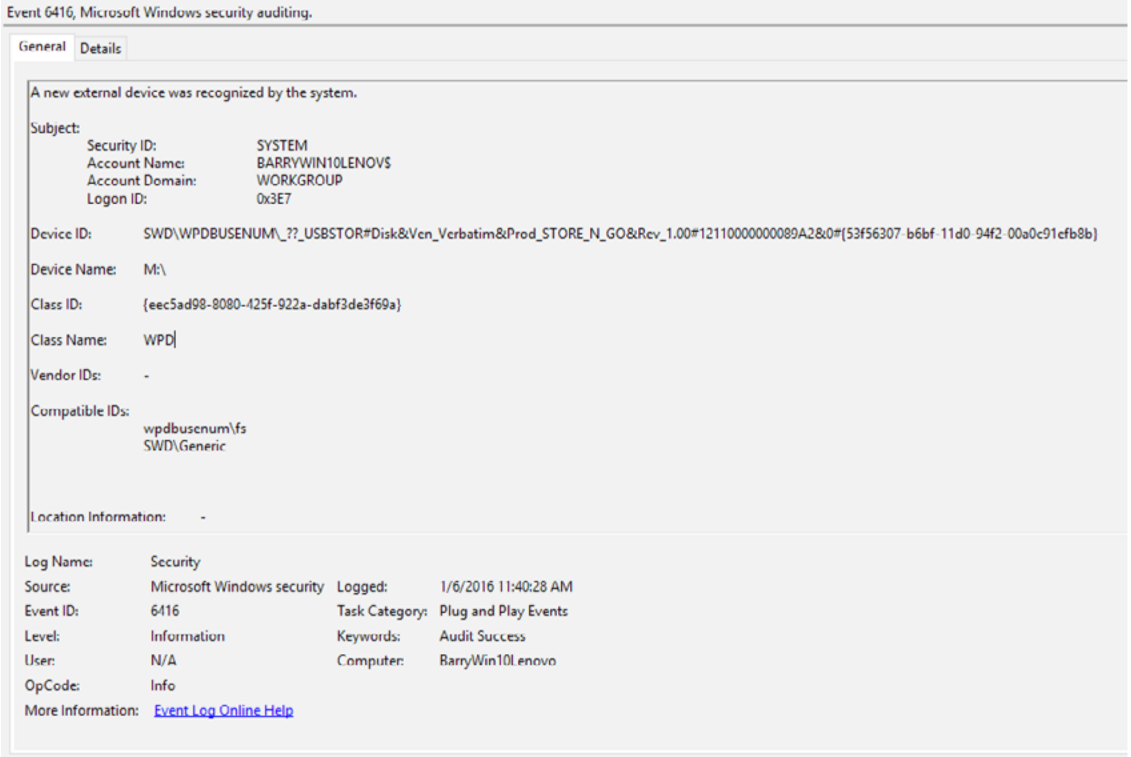
By knowing what a logon event looks like across multiple systems and vectors, you can build rules to analyze the data and find anomalies that might indicate an issue. Take the example of a brute force attack, in which logon attempts on a given system (or on multiple machines) are made using various passwords from different machines to hide the attack. By analyzing all logon events, not just those from one machine, you can quickly identify and receive notification of the attack.

USB/Plug-and-Play Device Connection

One way in which threat actors inject malware is through social engineering, which can include the use of USB devices. When you insert any kind of Plug-and-Play (PnP) peripheral—from USB stick, to camera, to everything in between—there has been very little ability to track that activity.

In previous version of Windows, the first time a device was inserted, an event was logged. When the device was removed and re-inserted, the repeated use of the device was not logged. The initial logged event was merely a record that a specific device with a certain serial number was first used on that system.

In Windows 10, a new category of Audit PnP Activity (found under Detailed Tracking) generates event 6416, shown in this figure. This event is generated each time an external device is recognized by Windows 10.



```
A new external device was recognized by the system.

Subject:
        Security ID:            SYSTEM
        Account Name:           BARRYWIN10LENOV$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Device ID:      SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_Verbatim&Prod_STORE_N_GO&Rev_1.00#121100000000089A2&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Device Name:    M:\

Class ID:       {eec5ad98-8080-425f-922a-dabf3de3f69a}

Class Name:     WPD

Vendor IDs:     -

Compatible IDs:
                wpdbusenum\fs
                SWD\Generic


Location Information:   -
```

```
Log Name:         Security
Source:           Microsoft Windows security   Logged:          1/6/2016 11:40:28 AM
Event ID:         6416                         Task Category:   Plug and Play Events
Level:            Information                  Keywords:        Audit Success
User:             N/A                          Computer:        BarryWin10Lenovo
OpCode:           Info
More Information: Event Log Online Help
```

LogRhythm MDI Insight

By tracking each instance of use of a PnP device and correlating that action with other events that indicate malicious activity, such as the launch of a malware process, the source of a malware infection—in this case, the implied use of a USB stick—can be tracked and identified.

Getting Started with What's New in the Windows 10 Security Log

All the new policies outlined in this paper are available on pre-Windows Server 2016 domain controllers. To access the Windows 10 policies, you must edit the Group Policy Object (GPO) from a Windows 10 system. If you edit the same GPO from an earlier operating system, you will not see those settings. Note that although you cannot see the settings from pre-Windows 10 or pre-Windows Server 2016 machines, even when you edit the same GPO from an earlier operating system, the Windows 10 policy settings are not overwritten or lost, allowing the same GPO to be applied to a mix of versions of Windows 10 and pre-Windows 10 systems.

LogRhythm MDI Insight

Don't simply jump into alerting on these new events. Instead, begin collecting the data from these new fields and events, and run a report to understand what is "normal" for your organization. After you've established a baseline, set up alerts for anything that falls outside of the norm.

Last, to ensure the most secure environment possible, require auditing and SIEM sensors on every Windows 10 workstation. Without these in place, threat actors can compromise a system that isn't auditing known potential threat actions, leaving a gap in your security.

Use the New Security Events in Windows 10 to Detect the Enemy

Despite some additional Group Policy categories and resulting events, the event log remains 99.9 percent unchanged. However, the detail provided in these small changes are materially beneficial to those organizations that seek to further strengthen their security stance when monitoring potentially risky activity on Windows 10 machines.

By enabling auditing of these new policy categories, and by centrally collecting and analyzing the resulting events, Windows 10 enables IT organizations to be aware of potentially threatening activity, maximizing the discovery of threat actions while minimizing the organization's risk.

About LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's award-winning platform unifies next-generation SIEM, log management, network and endpoint monitoring and forensics, and security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence.

Consistently recognized by third-party experts, LogRhythm was named a "Champion" in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report, awarded the SANS Institute's "Best of 2014" award in SIEM and received the SC Magazine Reader Trust Award for "Best SIEM Solution" in April 2015. Additionally, the company earned Frost & Sullivan's 2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award. LogRhythm is headquartered in Boulder, Colorado, with operations throughout North and South America, Europe and the Asia Pacific region.

About LogRhythm Labs

LogRhythm Labs is comprised of information security experts who hold a wide range of industry certifications (e.g., CISSP, CISA, CEH, etc.). Members have extensive experience as network architects, security analysts and compliance officers at multinational corporations, strategic federal entities and incident response consultancies. Labs members continue developing expertise by working with customers and partners to address their most difficult security and compliance challenges on a regular basis.

Customers benefit from Labs' research through LogRhythm's frequent Knowledge Base updates, which embed analytics-driven defense capabilities into our Security Intelligence Platform through several threat detection and compliance automation modules. These modules provide customers new and updated device support, geolocation data, AI Engine rules, lists, dashboards and Smart**Response**™ plug-ins. Learn more about LogRhythm Labs here.

About Randy Franklin Smith

Randy Franklin Smith is an internationally recognized expert on the security and control of Windows and AD security. Randy publishes www.UltimateWindowsSecurity.com and wrote The Windows Server 2008 Security Log Revealed—the only book devoted to the Windows security log. Randy is the creator of LOGbinder software, which makes cryptic application logs understandable and available to log-management and SIEM solutions. As a Certified Information Systems Auditor, Randy performs security reviews for clients ranging from small, privately held firms to Fortune 500 companies, national, and international organizations. Randy is also a Microsoft Security Most Valuable Professional.challenges on a regular basis.

Disclaimer & Copyright

Monterey Technology Group, Inc. and LogRhythm make no claim that use of this white paper will assure a successful outcome. Readers use all information within this document at their own risk. Ultimate Windows Security is a division of Monterey Technology Group, Inc.