**Rogue Processes**
Malware authors generally pick one of two strategies for obfuscating their malicious processes: hide in plain sight and attempt to appear legitimate, or use code injection and/or rootkit methods to hide from the view of normal analysis tools. See below for more on code injection and rootkits.

When searching for malware attempting to hide in plain sight, look for process names that appear legitimate but originate from the wrong directory path or with the wrong parent process ID. Look for suspiciously low memory usage, or having no exection and check for unusual command-line arguments. See the opposite side of this poster for legitimate Windows process details.

Besides processes, also look for suspicious DLLs executed through svchost.exe, implemented on a standard system is almost always worth looking into further.

**Unusual OS Artifacts**

**Unusual Services**
Windows services are designed to run applications in the background without user interaction. Many services are required on system boots, such as the RPC Client, Windows Firewall, Task Log, Server, and Workstation services. These services provide critical functionality for the OS and must be started immediately without requiring user input.

Services can be initiated using standard mechanisms accessible as named pipes, to name one. In order to consume resources, many services will self-start together and run under a smaller set of svchost.exe instances. svchost.exe is a Windows service that runs processes and it is typical to see several running instances of svchost.exe (5 or more is common).

Service configurations, as well as device driver configurations, are stored in the registry under HKLM\SYSTEM\CurrentControlSet\Services. This key holds every parameter for such service, including the service name, display name, path to the service's executable image file, start type, required privileges, dependencies, and more. Each service has a start type configured to start at boot, by manual intervention, or on trigger events such as obtaining an IP address or hardware device connection. Windows services provide great flexibility to developers, and similarly malware authors, for from writing malware and using a Windows service.

For offline analysis, investigate service configurations within the registry. On live or remote systems, use the built-in "sc" command to query installed services. Try parameters such as "scquery", "scopen", "scgetinfo", or "scquerytype" to get detailed information on service configurations.

**Unusual Network Activity**
Many care processes in Windows utilize the network, including svchost.exe, Iusus.exe, and even the svchost.exe process. Since you can't rule out the possibility of legitimate network activity from these processes, you need an effective way to identify deviations from typical network activity. With memory analysis, you can parse through memory and review residual connections and sockets established by the system. When you are just starting to try to identify unusual network behavior, keep an eye out for the following:

- Any process communicating over port 80, 443, or 8080 that is not a browser
- Any browser not communicating on ports 80, 443, or 8080
- Connections to unexplained external or internal IP addresses. For example, why did a process have a TCP connection to a system in Moldova?
- Web requests directed to an IP address rather than a domain name
- RDP connections (port 3389), particularly originating from odd IP addresses. External RDP connections are typically routed through a VPN concentrator.
- DNS requests for unusual domain names

In an intrusion case, spotting the difference between abnormal and normal is often the difference between success and failure. Your mission is to quickly identify suspicious artifacts in order to verify potential intrusions. Use the information below as a reference for locating anomalies that could reveal the actions of an attacker.

**Suspicous Network Activity**
Many care processes in Windows utilize the network, including svchost.exe, Iusus.exe, and even the svchost.exe process. Since you can't rule out the possibility of legitimate network activity from these processes, you need an effective way to identify deviations from typical network activity. With memory analysis, you can parse through memory and review residual connections and sockets established by the system. When you are just starting to try to identify unusual network behavior, keep an eye out for the following:

- Any process communicating over port 80, 443, or 8080 that is not a browser
- Any browser not communicating on ports 80, 443, or 8080
- Connections to unexplained external or internal IP addresses. For example, why did a process have a TCP connection to a system in Moldova?
- Web requests directed to an IP address rather than a domain name
- RDP connections (port 3389), particularly originating from odd IP addresses. External RDP connections are typically routed through a VPN concentrator.
- DNS requests for unusual domain names

In an intrusion case, spotting the difference between abnormal and normal is often the difference between success and failure. Your mission is to quickly identify suspicious artifacts in order to verify potential intrusions. Use the information below as a reference for locating anomalies that could reveal the actions of an attacker.

**Code Injection and Rootkit Behavior**

Typical code injection techniques provide an effective way to hide malware without relying upon low-level programming knowledge, thus making it a popular choice among malware authors. Code injection is almost never legitimate, so the existence of code injection in a registry key is usually a clear indicator. Finding evidence of code injection on a standard system is almost always worth looking into further.

A rootkit is a broad term for describing ways of subverting the operating system with the intent to hide activities and data. There are a number of techniques for doing this, but the end result is usually malware. Rootkits are signed by Microsoft for live response memory analysis, Mandiant's Persistent will check on-disk signatures for running code. For offline analysis, Ransomware Attribution Tools or Systeminfo Lightweight.exe provides a tremendous amount of information about a file digital signature.

**Unusual OS Artifacts**

**Unusual Network Activity**
Many care processes in Windows utilize the network, including svchost.exe, Iusus.exe, and even the svchost.exe process. Since you can't rule out the possibility of legitimate network activity from these processes, you need an effective way to identify deviations from typical network activity. With memory analysis, you can parse through memory and review residual connections and sockets established by the system. When you are just starting to try to identify unusual network behavior, keep an eye out for the following:

- Any process communicating over port 80, 443, or 8080 that is not a browser
- Any browser not communicating on ports 80, 443, or 8080
- Connections to unexplained external or internal IP addresses. For example, why did a process have a TCP connection to a system in Moldova?
- Web requests directed to an IP address rather than a domain name
- RDP connections (port 3389), particularly originating from odd IP addresses. External RDP connections are typically routed through a VPN concentrator.
- DNS requests for unusual domain names

In an intrusion case, spotting the difference between abnormal and normal is often the difference between success and failure. Your mission is to quickly identify suspicious artifacts in order to verify potential intrusions. Use the information below as a reference for locating anomalies that could reveal the actions of an attacker.

**Suspicous Network Activity**
Many care processes in Windows utilize the network, including svchost.exe, Iusus.exe, and even the svchost.exe process. Since you can't rule out the possibility of legitimate network activity from these processes, you need an effective way to identify deviations from typical network activity. With memory analysis, you can parse through memory and review residual connections and sockets established by the system. When you are just starting to try to identify unusual network behavior, keep an eye out for the following:

- Any process communicating over port 80, 443, or 8080 that is not a browser
- Any browser not communicating on ports 80, 443, or 8080
- Connections to unexplained external or internal IP addresses. For example, why did a process have a TCP connection to a system in Moldova?
- Web requests directed to an IP address rather than a domain name
- RDP connections (port 3389), particularly originating from odd IP addresses. External RDP connections are typically routed through a VPN concentrator.
- DNS requests for unusual domain names

In an intrusion case, spotting the difference between abnormal and normal is often the difference between success and failure. Your mission is to quickly identify suspicious artifacts in order to verify potential intrusions. Use the information below as a reference for locating anomalies that could reveal the actions of an attacker.

**Code Injection and Rootkit Behavior**

Typical code injection techniques provide an effective way to hide malware without relying upon low-level programming knowledge, thus making it a popular choice among malware authors. Code injection is almost never legitimate, so the existence of code injection in a registry key is usually a clear indicator. Finding evidence of code injection on a standard system is almost always worth looking into further.

A rootkit is a broad term for describing ways of subverting the operating system with the intent to hide activities and data. There are a number of techniques for doing this, but the end result is usually malware. Rootkits are signed by Microsoft for live response memory analysis, Mandiant's Persistent will check on-disk signatures for running code. For offline analysis, Ransomware Attribution Tools or Systeminfo Lightweight.exe provides a tremendous amount of information about a file digital signature.

**Unusual OS Artifacts**

**Unusual Network Activity**
Many care processes in Windows utilize the network, including svchost.exe, Iusus.exe, and even the svchost.exe process. Since you can't rule out the possibility of legitimate network activity from these processes, you need an effective way to identify deviations from typical network activity. With memory analysis, you can parse through memory and review residual connections and sockets established by the system. When you are just starting to try to identify unusual network behavior, keep an eye out for the following:

- Any process communicating over port 80, 443, or 8080 that is not a browser
- Any browser not communicating on ports 80, 443, or 8080
- Connections to unexplained external or internal IP addresses. For example, why did a process have a TCP connection to a system in Moldova?
- Web requests directed to an IP address rather than a domain name
- RDP connections (port 3389), particularly originating from odd IP addresses. External RDP connections are typically routed through a VPN concentrator.
- DNS requests for unusual domain names

In an intrusion case, spotting the difference between abnormal and normal is often the difference between success and failure. Your mission is to quickly identify suspicious artifacts in order to verify potential intrusions. Use the information below as a reference for locating anomalies that could reveal the actions of an attacker.

**Suspicous Network Activity**
Many care processes in Windows utilize the network, including svchost.exe, Iusus.exe, and even the svchost.exe process. Since you can't rule out the possibility of legitimate network activity from these processes, you need an effective way to identify deviations from typical network activity. With memory analysis, you can parse through memory and review residual connections and sockets established by the system. When you are just starting to try to identify unusual network behavior, keep an eye out for the following:

- Any process communicating over port 80, 443, or 8080 that is not a browser
- Any browser not communicating on ports 80, 443, or 8080
- Connections to unexplained external or internal IP addresses. For example, why did a process have a TCP connection to a system in Moldova?
- Web requests directed to an IP address rather than a domain name
- RDP connections (port 3389), particularly originating from odd IP addresses. External RDP connections are typically routed through a VPN concentrator.
- DNS requests for unusual domain names

In an intrusion case, spotting the difference between abnormal and normal is often the difference between success and failure. Your mission is to quickly identify suspicious artifacts in order to verify potential intrusions. Use the information below as a reference for locating anomalies that could reveal the actions of an attacker.

**Code Injection and Rootkit Behavior**

Typical code injection techniques provide an effective way to hide malware without relying upon low-level programming knowledge, thus making it a popular choice among malware authors. Code injection is almost never legitimate, so the existence of code injection in a registry key is usually a clear indicator. Finding evidence of code injection on a standard system is almost always worth looking into further.

A rootkit is a broad term for describing ways of subverting the operating system with the intent to hide activities and data. There are a number of techniques for doing this, but the end result is usually malware. Rootkits are signed by Microsoft for live response memory analysis, Mandiant's Persistent will check on-disk signatures for running code. For offline analysis, Ransomware Attribution Tools or Systeminfo Lightweight.exe provides a tremendous amount of information about a file digital signature.
Knowing what's normal on a Windows host helps cut through the noise to quickly locate potential malware. Use the information below as a reference to know what's normal in Windows and to focus your attention on the outliers.

When searching for malicious processes, look for any of these anomalous characteristics:

- Started with the wrong parent process
- Image executable is located in the wrong path
- Misspelled processes
- Processes that are running under the wrong account (incorrect SID)
- Processes with unusual start times (i.e., starts minutes or hours after boot when it should be within seconds of boot)
- Unusual command-line arguments
- Packaged executables

Process listing from Windows 7 Enterprise

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>winlogon.exe</td>
<td>Responsible for authenticating users by calling an appropriate Security Service Provider (SSP) and passing the credentials to Start Time: Winlogon loads the user's user's shell (i.e., explorer.exe)</td>
</tr>
</tbody>
</table>