Threat Detection with EventSentry

NETIKUS.NET ltd
Version 1.0.0

Overview

1 Overview

Malware poses an ongoing and growing challenge to governments, institutions, businesses and private individuals.

This guide offers insight into common practices and methods employed by threats of all kinds, including Malware & Ransomware.

EventSentry's real-time monitoring and detection features can help both prevent and detect many of these threats, which is are key to minimizing damage, preventing data loss and maintaining business continuity.

EventSentry detection methods are agnostic to specific types of malware, and accomplishes detection by monitoring hosts and networks from multiple vantage points.

1. **Real-Time Log Monitoring**
   - Anomaly Detection
   - Advanced Log Correlation (chains, timers, thresholds, ...)
   - File Integrity Monitoring (FIM)

2. **Ongoing Security Analysis**
   - Validation Scripts
   - Active Directory Inventory
   - Audit Policy Monitoring

3. **Inventory Monitoring**
   - Scheduled Tasks
   - Services & Drivers
   - Browser Extensions
   - Permissions
   - Software & Windows Patches
   - USB storage Devices

4. **Active Directory**
   - User, Group & Computer Inventory
   - Object Monitoring
   - Group Policy Monitoring

5. **Real-Time Security Dashboards**

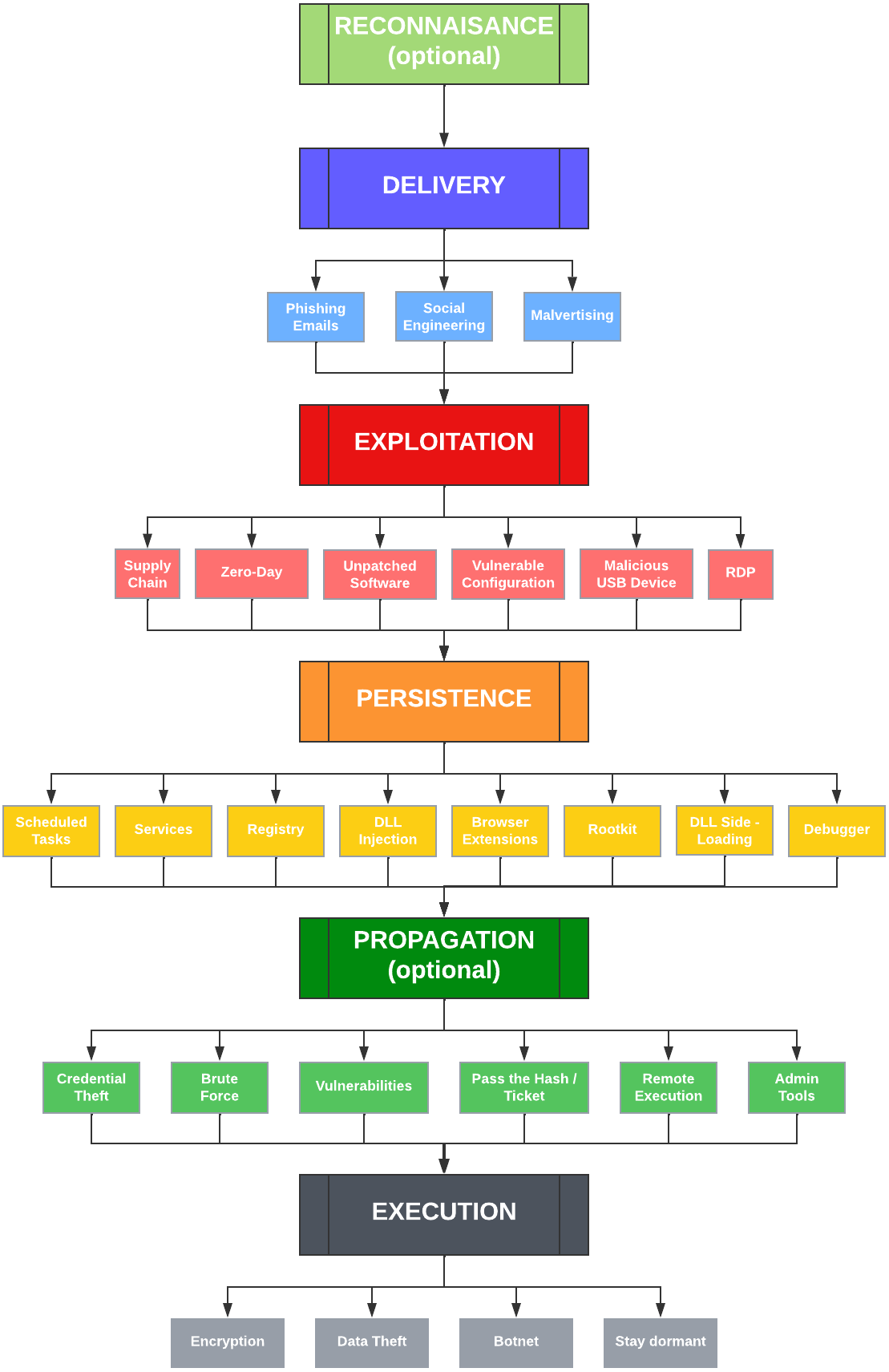
6. **Extensive Data Collection for Forensics**

7. **Enhanced Audit Reporting**
   - Process Activity (incl. Sysmon)
   - Network Logon Activity (incl. RDP)
   - File Access Activity

8. Network Traffic Analysis
- Observe traffic to/from malicious IPs
- Detect new hardware devices

While EventSentry (and other security products) may not detect every activity by malware, it's wide array of monitoring features usually flag at least one type of activity performed by Malware. It is however still essential to protect networks from multiple angles to reduce the attack surface in the first place, including:

- **User Education & Awareness**
  - Mitigates social engineering and phishing attacks
- **Email Security**
  - Mitigates phishing attacks
- **Firewalls & Perimeter Security**
  - Reduces attack surface
- **Patch Management**
  - Mitigates software and OS vulnerabilities
- **Antivirus Software**
  - Detects infections and known threats



Delivery

2 Delivery

Attackers utilize a variety of methods to deliver malicious software to a target system. The most common techniques to deliver malware are listed below.

Phishing Attacks
Attackers send fraudulent emails or messages that manipulate recipients into taking actions that ultimately allow for malware delivery.

Social Engineering
Attackers employ a variety of methods in order to convince the victim into taking action that gives them access to the target system. This includes impersonating trusted entities like IT support, colleagues, friends or authorities. Reconnaissance on social media is often an integral part, giving the attacker important information to carry out the social engineering attack.

Malvertising
Cybercriminals use malicious ads (e.g. job ads) which deliver malware when the visitor interacts them. These types of ads are either posted on legitimate web sites or delivered through ad networks that previously infiltrated.

Watering Hole Attacks
Though not common, attackers compromise web sites which are frequently visited by employees of a targeted organization.

Public Code Repositories (GitHub etc)
Cybercriminals infiltrate open source projects hosted on popular public code repositories, where they covertly inject their malicious code into popular software and scripts. Project maintainers - especially of larger projects containing hundreds of files - may not immediately notice this, since the malicious code blends in with legitimate code. Software developers then download and run the tainted code on their systems - giving the attacker essentially direct access to the software developer's workstation. In the worst case the developer distributes the code to customers, turning this into a supply chain attack.

Exploitation

3 Exploitation

Once the malicious software has been delivered to the target system in one way or another (web site, email attachment, ...), the malicious code executes and attempts to exploit a weakness in the target system to run successfully.

If the exploit is successful, the malicious code will execute and usually attempt the following:

- Create persistence to remain active even after a reboot, logoff etc.
- Propagate on the network to infect more systems. Since propagation carries the risk of easier detection, it is usually only done when it benefits the purpose of the infection (botnet, mining, ransomware, ...)
- Execute the payload to achieve the ultimate goal of the infection, for example encryption, data theft, mining (cryptojacking)

3.1 Supply Chain

The purpose of a supply chain attack is to run malicious code on

- networks that are otherwise difficult to penetrate
- rapidly infect a potentially large number of users/networks

This can be accomplished by hiding the malware in a legitimate software product. What is dangerous about a supply chain attack, is that it can potentially infect a large number of networks (which depends on the install base of the infected software product) while at the same time being difficult to detect if the malware manages to blend in with the legitimate software product.

Attackers can use a variety of methods to infiltrate a sotware product:

- Compromise the build environment & inject malicious code
- Manipulate dependencies (e.g. libraries)
- Compromise the build process
- Compromise the software distribution (e.g. download web site)

Software vendors are at risk for supply chain attacks, and need to take measures to prevent or at least detect these types of attacks.

3.2 Zero-Day

Zero-Day vulnerabilities are software flaws which are generally only known to a small number of security researchers and hackers. These vulnerabilities are sometimes exploited even before the software vendor is aware of them.

But even after they are fixed, deployment of patches to the entire user base may take a significant amount of time - giving attackers time to actively exploit them.

As such, if these vulnerabilities fall into the wrong hands - or when they have been discovered by threat actors in the first place - they can quickly cause havoc across entire infrastructures - which usually caught off-guard.

Since no signatures exist, only active monitoring with tools that use malware-agnostic methods like EventSentry can effectively detect these attacks in a timely fashion and prevent lateral movement and a large-scale infection.

3.3 Unpatched Software

Virtually all software products - including Operating Systems - encounter bugs throughout their lifetime. If these bugs are exploited before the software vendor fixes them or before a fix is applied, attackers can:

- Take advantage of the software's elevated privileges
- Gain access to unauthorized information inside the software product
- Gain access to the OS / network the software is installed on

It's important that a company has a coherent patch management solution in place, that ensures that all software and hardware is patched on a regular basis:

- Operating Systems
- Client Software
- Server Software
- Hardware Devices

EventSentry can help identify outdated Operating Systems and software products to ensure that all critical software is up to date:

EventSentry Benefits		
Windows OS Validation Scripts identify any Windows-based OS that is not on the latest patch level or EOL.		
DESCRIPTION	CONFIGURATION	REPORTING
Windows Patch Inventory Patch Monitoring shows all installed patches of a host and a history of all installed patches.		
DESCRIPTION	CONFIGURATION	REPORTING
Windows Software Software Monitoring tracks all installed software, version checks are done for common software.		
DESCRIPTION	CONFIGURATION	REPORTING

3.4 Vulnerable Configuration

Even when a software product is patched and on the latest version, an incorrect setup or configuration can still create vulnerabilities that can be exploited. This refers mostly to server-side software products, but can apply to client software products as well.

- **Default settings** in software products often don't prioritize security. Attackers can analyze popular software products and take advantage of this.
- **Insecure or default passwords** offer an easy way to for attackers to get unauthorized access to a software suite.
- **Unnecessary open ports** and **unnecessary features** increase the attack surface and may provide an additional attack vector.
- Similar to insecure passwords, overly permissive and **incorrect access control** may grant users unnecessary permissions.
- **No or insufficient logging** may make it impossible to detect configuration changes, failed logins and other critical activity.
- Other risks include missing security features, lack of encryption and other human errors

EventSentry Benefits		
Unnecessary Ports Port monitoring identifies new ports that applications are listening on. All open ports in the entire network can be queried to identify unnecessary TCP ports.		
DESCRIPTION	CONFIGURATION	REPORTING
Insufficient Logging Log files can be monitored in real time so that critical log data can be alerted on in real time.		
DESCRIPTION	CONFIGURATION	REPORTING

3.5 Malicious USB Device

Malicious USB drives provide an effective way to get direct access to computers inside a corporate network. Attackers may directly plug in the malicious USB devices into a computer in a public area (such as a doctor's office, bank, retail) or leave the USB drive in a public place (e.g. lobby, conference room, cafeteria) with the anticipation that an employee will plug in the device.

These types of attacks may also involve social engineering, where an attacker may pretend to be IT support personnel, contractor or an executive in order to gain some level of trust from the recipient and convince them that the device is harmless and can be trusted.

As is the case with social engineering, it's important that users are aware of these risks that allowing the attachment of USB devices is only allowed when necessary. At a minimum, usage of USB storage devices should be audited with Windows.

EventSentry Benefits		
Storage Audit Verifies that storage auditing in Windows is enabled on all endpoints, real-time event log monitoring stores and alerts on Windows audit events.		
	CONFIGURATION	REPORTING
USB Storage Inventory Attaching and removing USB devices is detected and alert on, (USB) storage devices are visible in the web-based reporting.		
DESCRIPTION	CONFIGURATION	REPORTING

3.6 RDP

RDP ("Remote Desktop Protocol") is a widespread protocol used on the majority of Windows devices, especially servers, and is frequently exploited by attackers. While not insecure by nature, attackers can exploit RDP in a variety of ways:

- Brute force attacks can be successful if the target system (and/or domain) does not have an account lockout policy in place. Brute force attacks will remain unnoticed if the target system does not have auditing enabled, and/or if audit events are not actively monitored.
- RDP may suffer from unpatched vulnerabilities, for example if the target system is running an older version of Windows or if Windows is not adequately patched.
- Man-in-the-Middle Attacks can be used to harvest user credentials
- RDP ports exposed to the Internet can also be used for information gathering, as the RDP protocol may divulge useful information about the target system.

To reduce your attack surface, never make RDP ports accessible to the Internet. If RDP has to be made available to untrusted networks, always change the default port, enable auditing and enforce account lockout policies.

Persistence

4 Persistence

Malicious software often intends to do damage over extended periods of time, for example when it:

- attempts to spread across the network
- slowly ex-filtrates data
- acts as a Trojan horse, waiting for further instructions

Persistence ensures that the malware survives system reboots, which is especially crucial on workstations. Achieving persistence naturally increases the risk of detection if the infected system is adequately monitored. As such, malware attempts to create persistence with methods that are not easily detected.

Windows-based malware utilizes a number of different techniques to achieve persistence, the most common methods along with detection mechanisms being documented here.

4.1 Scheduled Tasks

Registering a scheduled task is a popular technique to ensure that malware is always active for a number of reasons:

1. The creation/deletion of scheduled tasks is often not monitored
2. Malicious scheduled tasks may blend in with other legitimate tasks, due to the large number of scheduled tasks installed on modern Windows systems
3. Scheduled tasks can be scheduled to run in regular intervals, not just during a reboot
4. Regular users can create (limited) scheduled tasks

EventSentry Benefits

Task Scheduler Monitoring
Scheduled tasks can be monitored by both Windows and EventSentry, making it possible to detect suspicious changes in near real-time. For example, EventSentry supports comprehensive monitoring of scheduled tasks:

- The creation, deletion or change of any scheduled task can be logged to the event log, generating an alert
- A complete inventory of all scheduled tasks can be viewed in the Web Reports
- A history of all scheduled tasks changes is available in the Web Reports

DESCRIPTION CONFIGURATION REPORTING

It is however important to avoid alert fatigue since malware usually uses common names for its tasks in order to blend in and avoid detection, including:

- SystemUpdate
- AdobeUpdate
- JavaUpdate
- WindowsDefender
- TaskScheduler
- TaskHost
- UpdateService
- GoogleUpdate

4.2 Services

Similar to scheduled tasks, malware can create a service or driver to establish itself on the breached system. Services have the advantage of potentially running under the LocalSystem account, giving them access to even more resources then the local Administrator.

Just like with scheduled tasks, adding services is a popular method for malware to achieve persistence since:

1. The creation/deletion of service is often not monitored
2. Malicious services and drivers may blend in with other, legitimate services, due to the large number of services installed on modern Windows systems

EventSentry Benefits

Service Monitoring
Services and drivers can be monitored by both Windows and EventSentry, making it possible to detect suspicious changes in near real-time. For example, EventSentry supports comprehensive monitoring of services:

- The creation, deletion and change of any service can be logged to the event log, generating an alert
- A complete inventory of all services and drivers can be viewed in the Web Reports
- A history of all service changes (including status changes) is available in the Web Reports

DESCRIPTION CONFIGURATION REPORTING

4.3 Registry

Malware can utilize a variety of registry locations to achieve persistence, including the popular **HKLM\Software\Microsoft\Windows\CurrentVersion\Run** path which is designed to automatically start applications when a user logs on, usually apps you find in the system tray.

Unfortunately, the Windows registry includes dozens of registry paths where applications can register themselves, and changes made there often remain undetected.

EventSentry Benefits

Autorun Monitoring
EventSentry monitors multiple registry and file locations where applications can be registered to automatically start after a user logs on. Changes to these locations are detected in real-time for further investigation.

DESCRIPTION CONFIGURATION

4.4 DLL Injection / Side-Loading

DLL injection is a sophisticated and powerful method to stealthily execute malicious code. Here, Malware will attach to an existing (legitimate) process and load its own DLL into that process. The malicious code inside the DLL is then executed within the context of that process. DLLs can either be actively injected, passively loaded via Windows's AppInit registry settings, take advantage of the search order or by other means.

DLL injection/loading has the following benefits for the attacker:

1. Since no new process is launched, detection methods that look for new processes will not generate alerts
2. Operating within the context of another process, may give the malware access to sensitive information or additional privileges
3. DLL injection/loading may also give the malware persistence, if the malignant DLL is loaded automatically with the process

Security measures, such as code signing, can help mitigate this attack vector, but detecting malicious code in DLLs typically requires advanced tools and techniques, such as the Sysinternals Sysmon utility.

EventSentry Benefits
AppInit The Validation Script "Threat Intel: Persistence - AppInit DLLs" can identify insecure AppInit settings. DESCRIPTION CONFIGURATION
Anomaly Detection with Sysmon DLL injection can be detected by combining Sysmon's "ImageLoad" (event id 7) feature with EventSentry's event log anomaly detection functionality. By establishing a baseline of known DLLs (includes the full DLL path) which any given process loads, EventSentry can then alert on new DLLs which were previously not loaded by the process. DESCRIPTION CONFIGURATION REPORTING
Detecting unsigned DLLs with Sysmon Potentially malicious DLLs can be detected by combining Sysmon's "ImageLoad" (event id 7) feature with EventSentry's advanced event log content filter rules, which can verify the digital signature of a DLL file. An *unsigned* DLL that is loaded into a *signed* process can be a sign of an infection.

DESCRIPTION	CONFIGURATION

4.5 Browser Extensions

Browser extensions are a popular attack vector since they are widely adopted among users and are often neither restricted nor monitored. Attackers can either distribute extensions or attack legitimate extensions.

Even though modern browsers restrict browser extensions and their access to user data, user error or software bugs may give browser extensions access to user data, allowing them to spy on private data including usernames and passwords.

It's important to restrict the installation of browser extensions and monitor all installed browser extensions on a regular basis.

EventSentry Benefits

Web Browser Extension Inventory
EventSentry can inventory all installed browser extensions and also alert on all browser extension activity, such as extensions being added, updated or removed. EventSentry users can see all installed browser extensions (Google Chrome, Mozilla Firefox and Microsoft Edge are supported) on the entire monitored infrastructure in seconds.

DESCRIPTION CONFIGURATION

4.6 Debugger

Malware can achieve persistence without raising red flags by taking advantage of a seemingly harmless feature in Windows called **Image File Execution Options**, "IFEO".

This feature, mostly geared towards to Software Developers, allows the debugging of any process by immediately attaching a "debugger" when the requested executable is launched. Malicious actors may use IFEO to redirect the of a legitimate executable to a malicious one, effectively injecting code or executing arbitrary commands during the launch of a program.

EventSentry Benefits
Image File Execution Options The Validation Script "Threat Intel: Persistence - Debugger" can identify insecure Image File Execution Options settings.
DESCRIPTION CONFIGURATION

4.7 Rootkit

Rootkits are a type of malware that is particularly stealthy about remaining in the infected system, making it not only extremely difficult to detect but also very difficult - if not impossible - to remove.

Rootkits often don't follow patterns of other malware after infecting a system, and take advantage of little used and obscure Windows functionality that is not generally known to the industry. If a rootkit is able to manipulate and infect the Windows kernel, then it can remain completely hidden since its code (process, drivers, etc) will remain concealed and not be visible to monitor and/or AV software. Additionally, rootkits at the kernel level are potentially able to intercept network & keyboard data to stealthy steal usernames, passwords and other valuable data.

Nevertheless, for a rootkit to be successful, it still needs to infect a system in the first place and gain administrative rights. As such, it's extremely important to detect any abnormal behavior on a monitored system.

EventSentry Benefits

There is no specific feature in EventSentry that can detect a rootkit once it's installed, however EventSentry's extensive monitoring and detection capabilities can detect most malicious activity that will precede a rootkit installation. This includes:

- Anomaly Detection
- Sysmon support & integration
- Service & Driver Inventory
- Advanced event log analysis

Propagation

5 Propagation

Since the system which was first infected by malware may not necessarily be (the most) valuable, it will usually attempt to propagate within the network to fulfill its mission. In most cases propagation requires administrative rights to be effective, even if only on the compromised system (vs the entire domain). As such, most attacks in this section assume the attacker has administrative privileges.

For example, Ransomware will attempt to find as many hosts as possible where it can encrypt data, whereas state-sponsored spyware may spread in an attempt to elevate their privileges and ultimately gain access to more sensitive data.

Whatever the reason, one should assume that an infected system will rarely remain the only one. Consequently it's equally as important to protect the inside of a network as it is to protect & monitor the external perimeter of a network.

This section examines the most common methods malware employs to spread within the network, how to protect yourself, and how this can be detected with EventSentry.

5.1 Credential Theft

Malware may attempt to either obtain Windows credentials, stored usernames and passwords from web browsers or other credentials the user may have stored on the system.

Windows Credentials
If the malware can get access to additional Windows credentials then it may be able to spread inside the network. This can be done via memory scraping, credential dumping, the credential manager and other methods.

Web Browser Credentials
Malware may specifically target web browsers to obtain stored credentials. Many users save their usernames and passwords for websites in browser password managers, and malware can target these repositories. This is particularly valuable with high-value victims that may have access to important web sites. For example, attackers pollute open source projects and embed malicious code in testing suites that obtains browser settings, among other things nefarious behavior.

Keylogging
Malware can intercept all keyboard activity, potentially giving it full access to usernames and passwords from both internal and external resources.

Other
Pass-The-Hash attacks and browser session hijacking are other methods that can give malware access to remote systems without the actual usernames and password.

Organizations can use several approaches to protect against credential theft:

- Ensure that the OS and all applications are up-to-date with the latest version and patches
- Ensure that best security practices are used throughout the network
- Detect unusual network activity, such as unusual logins and applications executed
- Detect additional keyboard and driver installation

EventSentry Benefits
Validation Scripts EventSentry Validation Scripts ensure that all Windows installations are up to date and that best security practices are followed.
DESCRIPTION CONFIGURATION
Windows Software Software Monitoring tracks all installed software, version checks are done for common software.
DESCRIPTION CONFIGURATION REPORTING
Anomaly Detection Anomaly monitoring can detect & flag unusual process activity, e.g. flagging processes that have never before been seen on a particular host.
DESCRIPTION CONFIGURATION
Service Monitoring Services and drivers can be monitored by both Windows and EventSentry, making it possible to detect suspicious changes like newly installed drivers in near real-time.
DESCRIPTION CONFIGURATION REPORTING

5.2 Brute Force

Even though brute force attacks may seem somewhat antiquated and inefficient, they are still actively used and can be an effective way to gain unauthorized access to a system. Brute force attacks can be successful under a number circumstances:

Password Lockout & Auditing
Brute force attacks can only succeed if the authentication system where the logons occur (whether a web site, network device, server) does not lock out users after a number of unsuccessful logon attempts, or if account lockout is not enabled. It's also important that the system supports auditing and that auditing is enabled, so that invalid login attempts can be detected.

Credential Stuffing & Dictionary Attacks
Since attempting every possible combination of a password can be impractical even on modern systems, the attacker can use a (extensive) list of common passwords instead. These passwords can be taken from dictionary lists as well as from lists of previously stolen passwords ("credential stuffing").

Weak Passwords
System which allow weak passwords (e.g. short length, low complexity) are also susceptible to brute force attacks, especially if the systems also lack auditing and account lockout functionality.

EventSentry Benefits		
Validation Scripts EventSentry Validation Scripts ensure that all Windows domains and hosts have strong password policies and account lockout policies are enabled.		
DESCRIPTION	CONFIGURATION	
Syslog & SNMP Logs Failed authentication attempts from remote Non-Windows devices can be alerted on.		
DESCRIPTION	CONFIGURATION	REPORTING

5.3 Vulnerabilities

Similar to unpatched software in the exploitation phase, vulnerabilities in internal software can be take advantage of in order to gain access to remote systems.

It's important that a company has a coherent patch management solution in place, that ensures that all software and hardware is patched on a regular basis:

- Operating Systems
- Client Software
- Server Software
- Hardware Devices

EventSentry can help identify outdated Operating Systems and software products to ensure that all critical software is up to date:

EventSentry Benefits		
Windows OS Validation Scripts identify any Windows-based OS that is not on the latest patch level or EOL.		
DESCRIPTION	CONFIGURATION	REPORTING
Windows OS Patch Inventory Patch Monitoring shows all installed patches of a host and a history of all installed patches.		
DESCRIPTION	CONFIGURATION	REPORTING
Windows Software Inventory Software Monitoring tracks all installed software, version checks are done for common software.		
DESCRIPTION	CONFIGURATION	REPORTING

5.4 Pass the Hash / Ticket

This type of attack allows an attacker to authenticate against remote systems (usually Windows) without having the actual login credentials. Instead, the attacker obtains a (NTLM or Kerberos) hash from the compromised system and then uses this hash to authenticate against remote systems.

While these types of attacks are difficult to detect, they can be discovered from various different angles.

EventSentry Benefits		
Anomaly Detection Anomaly monitoring can detect & flag unusual logon activity, e.g. logons from a previously unknown user and/or IP address. Lateral movement across the infrastructure - which is usually a symptom of a pass-the-hash attack - can be detected with collector-side threshold filters.		
DESCRIPTION	CONFIGURATION	REPORTING
Detection suspicious behavior with Sysmon Certain Sysmon events can detect suspicious behavior, such as attempts to get access to the lsass.exe process.		
DESCRIPTION	CONFIGURATION	REPORTING

5.5 Admin Tools

Malware can leverage administrative tools and features within operating systems to propagate within a network. These tools - built into the operating system for legitimate system administration purposes - can be abused by malware to execute commands, spread across systems, and maintain persistence. This is also referred to "living off the land".

Attackers can utilize a number of utilities and features in Windows to spread inside a network. Utilizing existing tools that fall under the umbrella of administrative tools can offer significant functionality while at the same time blending in with regular administrative activity. However, several proactive and reactive steps can be taken to minimize this risk.

- Disable all unnecessary administrative features that aid attackers, for example WinRM
- Uninstall unneeded and unused software, including administrative tools and utilities
- Enforce the principle of least privilege
- Use LAPS or similar solutions to avoid password reuse
- Enable firewall rules on workstations to prevent peer to peer access (workstations rarely need to access each other)

EventSentry Benefits		
Anomaly Detection EventSentry can detect & flag unusual usage of administrative tools (and other executables), logon activity related to lateral movement and more.		
DESCRIPTION	CONFIGURATION	REPORTING
Validation Scripts Validation scripts help companies improve their baseline security by flagging insecure protocols, services and settings. Custom validation checks that are specific to the end user's organization can easily be integrated into built-in validation scripts.		
DESCRIPTION	CONFIGURATION	REPORTING
Windows Software Software Monitoring tracks all installed software and can help identify unneeded software.		
DESCRIPTION	CONFIGURATION	REPORTING

Execution

6 Execution

The last and most important phase of a malware attack is the execution phase, where the malware carries out its intended actions. Consequently, the type of execution depends on the intentions of the malware.

Malware can only reach the execution phase if it is not detected or repelled during earlier stages. If malware is able to reach the final execution phase, then it is important to detect the malicious software as quickly as possible so that the potential damage can be contained.

6.1 Encryption

Ransomware will attempt to encrypt critical files, databases and other valuable data while at the same time attempting to delete all available backups so that it's difficult or impossible for the victim to restore the data.

Ransomware will attempt to avoid detection until the encryption process is complete and the victim is presented with the dreaded message, explaining that only paying the ransom will give the victim access to the data again. Fast detection of a Ransomware infection is of utmost importance.

While detecting the actual encryption process in a timely fashion is difficult, extensive monitoring of the infrastructure can reveal that suspicious activity is underway and should be investigated asap. Detecting and responding may help mitigate the damage.

- Always make sure that backups of all critical data exists and cannot easily be tampered with, restore operations should be tested on a regular basis
- Auditing access to important files and directories can reveal unusual patterns, such as a high rate of file read/write access
- Unusual patterns in CPU usage may indicate that encryption is underway

EventSentry Benefits		
File Auditing Setting up NTFS Auditing for write access on critical files and monitoring for excessive activity can help detect Ransomware.		
DESCRIPTION	CONFIGURATION	REPORTING
File Entropy Since encrypted files tend to have a higher entropy than plain text files, alerting on high entropy can help detect Ransomware.		
DESCRIPTION	CONFIGURATION	REPORTING

6.2 Data Theft

Data theft can be similar to Ransomware attacks, where the attackers download confidential business data with the threat of releasing that data to the public if a ransom is not met. Data theft can also be an effort to steal specific data - for example industrial espionage by a competitor or nation state that is looking to steal intellectual property or customer data.

Data theft is difficult to detect, especially if the attacker obtains (or has) the credentials of a user with legitimate access to confidential data. Confidential data that is spread in multiple locations (e.g. file system, cloud, database, ...) may further complicate detection efforts. Some ways to detect data theft are:

1. Network traffic monitoring may reveal unusual patterns, but detecting this in busy networks can be extremely difficult - especially if the attacker leaks the data slowly over extended time periods.
2. Anomaly detection may also detect unusual patterns, such as read access to confidential data at unusual times or from unusual sources. But a sophisticated and careful attacker will not deviate from his/her usual pattern and as such may not trigger any anomaly alerts.
3. Email security monitoring can be an important component if the attacker has to use email to ex-filtrate the data.

User Behavior Analysis is likely the most effective way to detect targeted data theft, for example:

- Data is read by a user who does not normally access the data
- User accesses confidential data more frequently then usual
- User accesses data at an usual time of day

6.3 Botnet

When the purpose of the malware is a botnet, then the malware will usually attempt to spread on the compromised network and receive instructions from a C2 (command & control) server.

Bots become part of a larger botnet and will participate in various malicious activity such as:

- DDos attacks
- Spam Distribution
- Click fraud
- Crypto mining

Detecting botnets may be difficult if the bot activity is not too aggressive. However, since the whole purpose of the bots is to participate in malicious activity, activity monitoring is often the most effective way to discover anomalies:

- Network Activity
- Unusual resource usage on endpoints (e.g. CPU)

Even though the detection speed of botnets is not as critical as it is with Ransomware, it is nevertheless important to remove botnets as soon as possible to avoid further infections and damage.

6.4 APTs / Staying Dormant

When the purpose of the malware is a botnet, then the malware will usually attempt to spread on the compromised network and receive instructions from a C2 (command & control) server.

APTs are sophisticated and targeted cyber attacks conducted by well-resourced and highly skilled adversaries, often with specific objectives such as espionage, data theft, or long-term disruption.

APTs may remain dormant for extended periods of time, waiting for instructions from a C2 server. For example, a nation state may infect infrastructure providers and use the APTs to disrupt operation during a war or political event.

Detecting APTs that remain mostly dormant is extremely difficult, since the malware usually blends in with regular system activity. The most effective way to detect APTs is to prevent their installation in the first place and perform regular system audits that can identify irregular applications and services.

- A -

- B -

- C -

- D -

- E -

- F -

- I -

- K -

- L -

- M -

- N -

- P -

- R -

- S -

- T -

- U -

- V -

- W -

- Z -