Monitoring for indicators of ransomware attacks

Ransomware has been a problem for years but has recently gained visibility due to some high profile attacks. Briefly, ransomware is a form of malware designed to encrypt files on a device making them unavailable. Malicious actors then demand ransom in exchange for decryption keys. Depending on the nature of the files, this attack can establish widespread denial-of-service and extortion for a company or targeted individuals. You operate under the assumption that a breach will occur and that early detection is the key to minimizing the damage. You want to use Splunk Enterprise Security to search for potential vulnerabilities, look for system behavior that indicates ransomware is present, and contain any found ransomware before its goal of encryption can be achieved.

In general, ransomware prevention and detection has multiple parts that involve people process and technology. These include:

- Use antivirus software at all times
- Keep all computers fully patched
- Use security products or services that block access to known ransomware sites
- Configure operating systems to only allow authorized applications
- Promote awareness about security across the organization
- Monitor and investigate suspicious behaviors observed in the environment

Splunk comes into play with the last bullet. Splunk Enterprise Security helps you ingest, monitor, investigate/analyze and act (IMIA) on security data and insights. Early detection is directly related to your ability to monitor and investigate.

Ingest

Ingest is the foundation, and a best practice in security is to aggregate all your data in one central place so that disparate events on disparate devices and systems can be correlated. This consolidation is important to getting a full view of your environment. It is a little like having all the surveillance cameras displaying their views on a cluster screens that are monitored by security guards. Having all the logs in one place serves the same purpose in the digital world of
cyber security.

Endpoint data is the most essential data type needed to monitor for ransomware. Endpoints in this context refers to desktops, servers, laptops, virtual machines, containers, mobile devices, and more. The endpoint is often where an attack begins. Many of these endpoints contain rich data that must be monitored and mined to detect a ransomware attack. The endpoints that are targeted by ransomware contain files that are important to the business. That implies a known set of devices.

The types of data to be monitored are:

- User data, process data
- File create, read, update, delete (CRUD) events
- Registry and services CRUD
- Memory
- Device drivers
- Disk and network IO
- Metadata, including integrity checks and alerts, hash values, and similar

Additional data may be needed as new ransomware techniques are found.

Some important sources of evolving data are:

- [Windows event logs](#)
- [Windows Sysmon](#)
- Osquery
- [Antivirus data](#) from products such as Blue Coat, Crowdstrike, Symantec, FireEye, Tripwire, and others
- [Web proxy data](#)

Other sources could be needed but the list above represents the most common.

Getting endpoint data into Splunk involves the use of CIM compliant data via add-ons or Technical Adapters (TA) in combination with universal or, occasionally, heavy forwarders. See the documentation titled [Data source planning for Splunk Enterprise Security](#) for more details. You should also reference the [Getting Started with Enterprise Security article](#) for more information.

**Monitor**

After the security data is in Splunk Enterprise Security and populates the data models, monitoring begins with building, enabling, and running correlation searches that take action when system behavior looks like ransomware or when system or process vulnerabilities are found. Actions include:

- assigning a risk score
- raising an alert called a notable event for an analyst to triage and investigate
- forwarding to SOAR for further investigation and or automation

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
other configurable actions such running another relevant script or program

**Threat intelligence**

The prerequisite to building correlation searches, which are also called detections, is to know what to look for in the data. That starts with knowing what steps and behaviors ransomware attacks take and how this behavior presents itself in the data. Be aware that threat actors are always developing new ways to gain access, elude detection, establish persistence, and impact systems. That means you must rely on timely threat research that comes from various places, including Splunk's threat research team (STRT).

Knowing what to look for begins with knowing the tactics and techniques used by adversaries. Collectively this is known as gathering threat intelligence. A popular framework for threat intelligence is MITRE ATT&CK, a knowledge base of observed threat behaviors collected from many sources throughout the cyber security community. The content in ATT&CK is constantly evolving as new techniques are discovered. This is a key reason why you must develop a process around using threat intelligence to develop and refine your detections and to stay current. ATT&CK is a good place to start, but there are other frameworks as well that include the Lockheed Kill Chain and the NIST CIS controls.

In addition to the frameworks, there are groups called Information Sharing and Analysis Organizations or Centers (ISAO or ISAC). These groups further share threat intelligence to help keep up with the rapid development of techniques used by adversaries. See the content on Splunk Intelligence Management (SI) (formally TruSTAR) for more information on how to incorporate threat intelligence from these sharing groups into Splunk Enterprise Security.

Here are some links for further reading around threat intelligence:

- Docs: Splunk Security Essentials (SSE)
- Docs: Enterprise Security Content Update (ESCU)
- Tech Talk: Splunk Intelligence
- Lantern: Splunk Intelligence Management
- Blog: CISA's known Exploited Vulnerabilities Catalog and Splunk (ESCU)

**Correlation searches and continuous improvement**

Splunk Enterprise Security has many out-of-the-box correlation searches that can help you get started, but those are only a subset of what is available or what you might need. There is a larger and growing number of correlation searches available to you so that you can expand your detection coverage. These additional detections are developed by the Splunk Threat Research team (STRT) and are delivered to ES through the ES Content Update app and found in the use case library. The detections are mapped to threat techniques found in MITRE ATT&CK. As of today, you must manually update ESCU to get the latest content from STRT, but updates will be automatic in a future release of Splunk Enterprise Security.

Another place to find detections (sometimes called use cases) is in the Splunk Security Essentials app (SSE). SSE is a knowledge base and content development tool with some assistance for deployment. It is not however a fully operational tool like ES. SSE automatically updates its content from the STRT and maps to MITRE ATT&CK, similar to the ESCU app.
We recommend that you install Splunk Security Essentials (SSE) and the ES Content Update (ESCU) apps to assist with expanding correlation search coverage. Splunk Enterprise Security is the operational platform that gives you necessary components such as:

- notable events
- the assets and identities framework
- risk-based alerting and incident review
- dashboards
- the adaptive response framework for integration with other components and workflows.

Splunk Security Essentials helps you do security content development, and Splunk Enterprise Security helps you run security operations. An example of using SSE for content review and introspection is shown below. The chart is a screenshot from the SSE Analytic Advisor dashboard showing the MITRE techniques with detection coverage. Anything that is blue has detections written, with the darker the shade of blue indicating more detection coverage for that technique. The dashboard has good filtering capabilities to narrow down the detections that are recommended based on parameters such as threat group, data, and technique. You can see the filter options across the top.

Example of monitoring for indicators of ransomware attacks

To get specific detections for ransomware, use the Security Content > ATT&CK-Driven Content Recommendations dashboard and filter for the ransomware category. The result is an SSE matrix mapping back to MITRE with detailed description of the detections, what maturity stage they are in, what target apps they can run, and more. Each card in the Content list can be expanded to show more information on data sources, other frameworks, and guidance on how to implement.
Next, we will select a detection we to deploy. The following screenshot shows the detail of the Deleting Shadow Copies detection, which was one of the detections listed on the previous screen. When you select that detection from the previous screen, it presents the detail shown below.

Across the top is a description. Below that on the left you find information on how to implement, known false positives, and a pointer to sample data to experiment with. On the right is information on the frameworks, and if you hover over the colored boxes, you can get further details for each.

Note that the information on false positives is valuable when considering techniques for dealing with noise. You may decide to build a lookup to suppress events with known safe indicators or assign a risk score and put it into the risk index associated with the host. After the risk score hits a threshold, you make it a notable.

The rest of a detection page in Splunk Enterprise Security shows information on prerequisites, such as required macros and data. In this instance, we are missing some data but we are told what is missing and how to get it.

On the live application, you can hover over the colored boxes and get details about the tactics, techniques, and phases. On the bottom you can see the SPL of the search and other, related detections. This is everything you need to evaluate, further develop, and deploy the detection to Splunk Enterprise Security when you are ready.
After you have decided that this is a detection you want to implement, you can click the **Edit Scheduled Search** button and if it is content already in the ESCU app, then you can deploy it into the Splunk Enterprise Security instance from there. If not, you can try to update the ESCU app to pull it down.

If the detection is not in ESCU either but this is detection you would like to evaluate further, then you can run it in Splunk Security Essentials until it is ready for production or bring it to Splunk Enterprise Security and deploy it. To run it in Splunk Enterprise Security as a correlation that is not in ESCU, you can deploy it to ES Correlation Search editor. The following screenshots give an overview of the flow.

First, navigate to **New Content Configuration > Content Management** and select **Correlation Search** under the Create New Content button.

In the correlation search editor, give it a name. We recommend you give it a name that indicates it is under development with **dev** as a prefix, for example, dev-0.1.0-trg.

Enter a description and copy the search from Splunk Security Essentials into the search using Manual mode. In the

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
annotations field, enter the Mitre technique identifier or, if using a different framework, the appropriate identifier. SSE helps put all information in one place, making it a good development environment and complement to Splunk Enterprise Security.

Finally, you will need to configure the scheduling, throttling, and adaptive response settings for the search. For more information, see Configure correlation searches in Splunk Enterprise Security.

When the search is configured, ideally you would have a Red team activity simulate the technique on a canary system and make sure the detection works. If you have too much noise from production systems, you need to figure out how to eliminate the false positives. The Process.user may need to be added to a list of safe users or some similar element that signifies safe use of these commands. That is part of the development process.

Results

Being able to start with threats in a framework like MITRE, map them to detections that the Splunk Threat Research Team (STRT) has built goes along way toward getting the right ransomware monitoring in place. Frameworks decrease the amount of work you have to do, often down to tuning and adjustments to fit into your environment. This kind of start should greatly accelerate and expand your detection coverage. After you have one detection working well, it is time to configure more so that your coverage expands.

There are currently 368 results returned from a search on ransomware at the STRT github site! You could need to implement many of these detections in order to get comprehensive coverage for ransomware. The monitoring coverage is automated by scheduled searches and are surfaced to the SOC by notable events. In order to scale your scans...
(sweeps) that look for indicators of attack these detections are designed for, you need to use accelerated data models and the tstats command. The reason is that these are is typically 7-10 times faster then straight SPL against indexes. While it easier to use straight SPL to build your own detections, it will not scale. By leveraging the detections from the STRT, you will have much better coverage and alignment to known threats and most of the search work is already done.

Next steps

- Blog: Five questions your organization must ask to prepare for a ransomware attack