Rorschach Ransomware Analysis with Attack Flow

medium.com/@simone.kraus/rorschach-ransomware-analysis-with-attack-flow-7fa5ff613a75

Simone Kraus

April 19, 2023

Simone Kraus

--

How the online attack flow builder can be used for reverse engineering and forensics.

Curious about the new ransomware, which officially caused a sensation in the community for the first time last week under the name Rorschach, I wanted to know how the online attack flow builder can be used to design the attack flow from a reverse engineering and forensics point of view. Would it be possible? And what should I say? I'm not sure if everything is 100% implemented, but it helped me as an analyst to understand the Ransomware.

So I tried the experiment to graphically display the analysis in Attack Flow another great tool developed by the Center for Threat Informed Defense.
Attack Flow is an open source tool to graphically display and understand attacks in their

sequence.

Attack Flow website MITRE Engenuity: it helps defenders and leaders understand how adversaries operate and compose atomic techniques into attacks to better understand defensive posture.

> Attack Flow Builder is a free and open source tool for creating, viewing, and editing Attack Flows. This web-based tool provides a workspace where you can populate information about adversary actions and additional context, then weave those items into a flow by drawing arrows to indicate the sequences of adversary techniques observed during an incident or campaign.

Those who have previously had contact with event-oriented process chains or object-oriented programming will also become familiar with Attack Flow relatively quickly.
While there is an online version that you can use right away, you can also download the tool from github and install it on your virtual machine.
After I had first modeled the ransomware group Play as an attack flow, I now wanted to know how Rorschach — also known as BabLock — works and which MITER ATT&CK techniques are behind it. While at Play, for example, the CTI reports also describe the tools used by the ransomware group and you can then go deeper into detection engineering and threat hunting with the help of threat intelligence platforms such as Tidal, there are still relatively few information in the web about from BabLock.

Cortex XDR Dump Service Tool with cydump.exe can be used to load untrusted dynamic link libraries (DLLs)
Luckily today Trendmicro released an analysis about the ransomware. Perfect timing!

Although the ransomware was detected as a variant of LockBit, it cannot be clearly assigned to the LockBit group. Trendmicro refers to it as a “Frankenstein-like creation” of different ransomware solutions, however, Rorschach is the fastest variant of encryption ever seen and the automation also seems to be more advanced.
While I initially assumed an analysis similar to that of Play, it quickly became clear that using Attack Flow can also be used as a kind of assessment for threat actors, malware and where the attacks happened (location).

Short Assessment of the threat actor, the ransomware and where the unkown threat actor operates
The more I dived deeper into the ransomware itself, the more I realized that Attack Flow is an excellent reverse engineering and forensic tool. If you really want to understand the attacks in terms of the components of the artifacts a specific attack has, the representation of processes and procedures within it, attack flow can help you to understand the necessary technical understanding you’ve missed before. The analyst is more forced to understand the technical processes and more important: to understand them in the right order.

Command lines can be displayed just like files or software, as well as tools that can be pictured and sketched separately. The longer I spent time with Attack Flow, the more enthusiastic I am about it.

Command lines, files, processes and action can be added to have the whole overview of the procedures adversary use
I worked through the Trendmicro report step by step and realized that if I had only read the CTI report, half of the information would have been skimmed, but the technical depth for the ransomware itself only emerged during the modelling itself.

Using attack flow helps you understand the how the ransomware is deployed without having reversed engineered it on your own
Conclusion: I recommend every organization to familiarize themselves with such modelling tools and to study attacks graphically shown in a flow chart. Creating an attack flow not only helps to understand the correct course of the attack, but also to understand the technical depth that is necessary in order to then be able to write detection or make statements about which MITRE ATT&CK techniques are particularly relevant in order to achieve the fastest possible so called "choke point". It means to find an early MITRE ATT&CK technique in the kill chain where the attacker can't get any further.

For those who write forensic reports it can then be used as existing attack flows to verify own analysis hypotheses and have a basis for own documentation of the incidents. Even artifacts and IOCs can be mapped.

Basically, Attack Flow is a simple to use tool that is accessible to everyone, with which playbooks or threat hunting solutions can also be created.

> CTI analysts can use Attack Flow to create highly detailed, behavior-based threat intelligence products. The langauge is machine-readable to provide for interoperability across organizations and commercial tools. Users can track adversary behavior at the incident level, campaign level, or threat actor level. Instead of focusing on indicators of compromise (IOCs), which are notoriously inexpensive for the adversary to change, Attack Flow is centered on adversary behavior, which is much more costly to change.

AttackIQ's Breach and Attack Simulation tool goes one step further. It integrates the attack flows into the BAS solution and you can then emulate the attack modify steps and define different or several choke points as appropriate mitigations are implemented and tests are repeated iteratively, structured, rigid and measurable, rapidly. They've got a blog for the community where you can get the latest attack flows that AttackIQ has developed.

What's next? It would be interesting how to use such reverse engineering attack flows to develop further countermeasures or detections. D3FEND and other threat informed tools could provide to understand the adequate mitigation an organization need.

File Removal of known malicious artifacts could be an adequat countermeasure

Defensive Posture

The blue team can use Attack Flow to assess and improve their defensive posture, as well as provide leadership with a data-driven case for resource allocation. Attack Flow allows for a realistic risk assessment based on observed adversary sequences of attack, allowing defenders to play out hypothetical scenarios (e.g. table top exercises) with high fidelity. Defenders can reason about security controls over chains of TTPs to determine gaps in coverage, as well as choke points where defenses should be prioritized.

Executive Communications

Front-line cyber professionals can use Attack Flow to roll up highly complicated, technical details of an incident into a visual depiction that aids communication with non-technical stakeholders, management, and executives. This format Attack Flow allows defenders to present their analysis of an attack and their defensive posture strategically while de-emphasizing raw data, technical jargon, and other information that executives do not need to make a business decision. Defenders can use flows to communicate the impact of an attack in business terms (i.e. money) and make a convincing case for new tools, personnel, or security controls to prioritize.

Lessons Learned

Incident responders can use Attack Flow to improve their incident response (IR) planning and after-action review. After a security incident has occurred, responders can create flows to understand how their defenses failed and where they can apply controls to reduce future risk and enhance threat containment. Mapping a flow will also allow defenders to see where their defenses succeeded and what they should continue to do going forward. Creating attack flows is an easy way to ensure the incident is documented and organizational knowledge is retained for future use. Over time, this will improve defenders' ability to mitigate and recover from incidents more efficiently.

Adversary Emulation

The red team can use Attack Flow to create adversary emulation plans that focus their security testing on realistic sequences of TTPs informed by public as well as proprietary intelligence. The red team can leverage a corpus of attack flow to identify common attack paths and TTP sequences. In purple team scenarios, a flow is a very precise way to communicate between attackers and defenders.

Threat Hunting

> Threat hunters can use Attack Flow to identify common sequences of TTPs observed in the wild, then hunt for those same TTP chains in their own environment. These flows can guide investigative searches, piecing together techniques and timestamps to construct detailed timelines. Attack Flow can showcase the adversary tools and TTPs that are being used, which can help aid in writing detections against common behaviors and/or adversary toolsets, as well as prioritizing those detections.

An introduction to the Attack Flow project you can find here.