LogRhythm™

Using the MITRE ATT&CK® Framework to Boost Ransomware Defenses

Contents

01

Introduction

The explosive growth, evolution, and success of ransomware over the past few years has given rise to more and more cybercriminal gangs going the route of Ransomware as a Service (RaaS). Mirroring the normal business sector, we're seeing a separation of duties unfold, which is yielding a best of breed scenario for both development and execution. Traditionally, the people that are really good at developing ransomware, aren't necessarily so good at executing it, and vice versa. However, with the RaaS model, both parties are able to focus on what they do best. The result, of course, is that the threat to businesses is growing as the cybercriminal gangs are becoming more effective and taking millions of dollars in ransoms.

Over the past few years, two specific variants of RaaS — REvil and Conti — have been behind some of the most widespread and successful cyberattacks. In July of 2021, REvil hit the headlines when a group of Swedish grocery stores was hit with a ransomware attack, which was traced back to a supply chain attack at U.S. IT firm Kaseya. Before their shutdown through efforts by the U.S. Government, REvil was making claims of generating $100 million in profits annually. Conti started Google trending in June of 2020 but had its time in the limelight in May of 2021, when the Irish Health Services was hit by a ransomware attack. It's assumed Conti is making as much profit as REvil — if not more.

Putting aside REvil's supposed demise, looking at how REvil and Conti function during an attack can provide insight into what security teams should expect from most ransomware variants; analysis of both variants shows that the code in the software is very similar to previous variants, so while the names and players may change over time, the techniques being used in the attacks are the same, and this helps us in identifying and ultimately intercepting an attack.

This paper will use the MITRE ATT&CK® Framework, specifically looking at some of the tactics, techniques, and procedures (TTPs) used by REvil and Conti to explore how they impact organizations and hold them for ransom.

LogRhythm Insights — Detecting Ransomware Activity with LogRhythm

No security solution can guarantee stopping ransomware attacks. So, it's critical to have centralized visibility of all activity and changes within your entire environment that may serve as leading or active indicators of a ransomware attack.

Look for insights in this paper from LogRhythm and examples of how their security operations solution helps to detect and provide detail around ransomware attacks.

The MITRE ATT&CK® Framework

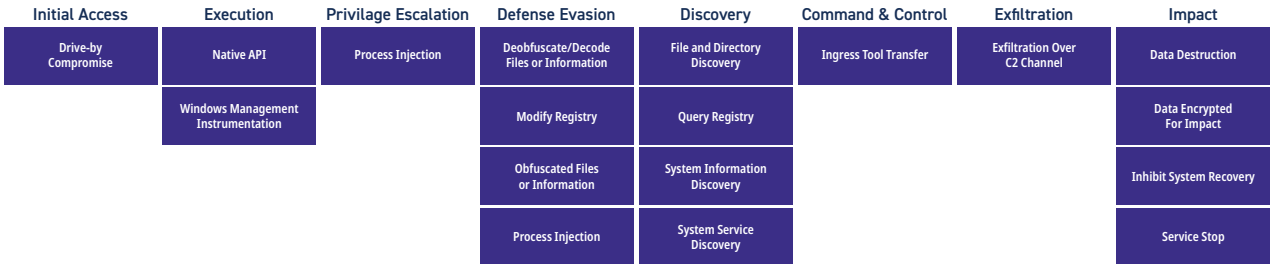
If you're not familiar already with the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework, it is an open framework and knowledge base of cyberattack tactics and techniques that reflects the different phases of an attack lifecycle, the types of actions taken, and the platforms they are known to target. Found on the web at attack.mitre.org, the framework allows you to search and navigate through the different types of attack techniques, which can be used to enhance, analyze, and test your threat hunting and detection efforts.

Zeroing in on REvil and Conti, MITRE provides comprehensive details about the TTPs used by these ransomware strains.

REvil

https://attack.mitre.org/software/S0496/

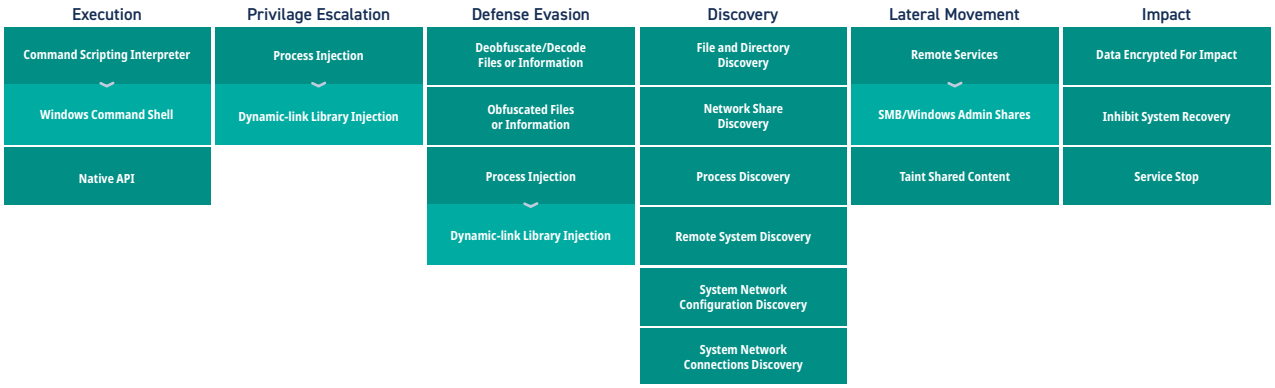
MITRE provides insight into the specific actions taken by REvil, from initial access all the way through encryption and stoppage of impacted services. Below is a highlighted example of those parts of the ATT&CK Framework that are applicable to REvil:



Conti

https://attack.mitre.org/software/S0575/

In the same way as with REvil, MITRE provides visibility into the equivalent actions taken by Conti during an attack. Note below how different Conti's techniques look from that of REvil above:



For the purpose of this paper, we will focus on two specific techniques that are shared techniques between the two ransomware variants, found under the Impact set of tactics:

- T1486: Data Encrypted for Impact
- T1490: Inhibit System Recovery

LogRhythm Insights—Strong Security Requires Comprehensive Visibility

When you're detecting and responding to threats, SOC Teams, Blue Team members, as well as IT and Security pros all need not only details, but also actionable insight that comes from seeing as close to everything that is occurring on the network as is possible.

LogRhythm helps to track and trace threat activity from a wide range of data sources. The example below shows activity detail specifically involving MITRE ATT&CK® T1486. With this degree of visibility, responders can quickly understand scope, triage and prioritize response activities, and focus efforts on where they will have the greatest impact to stop a ransomware attack.

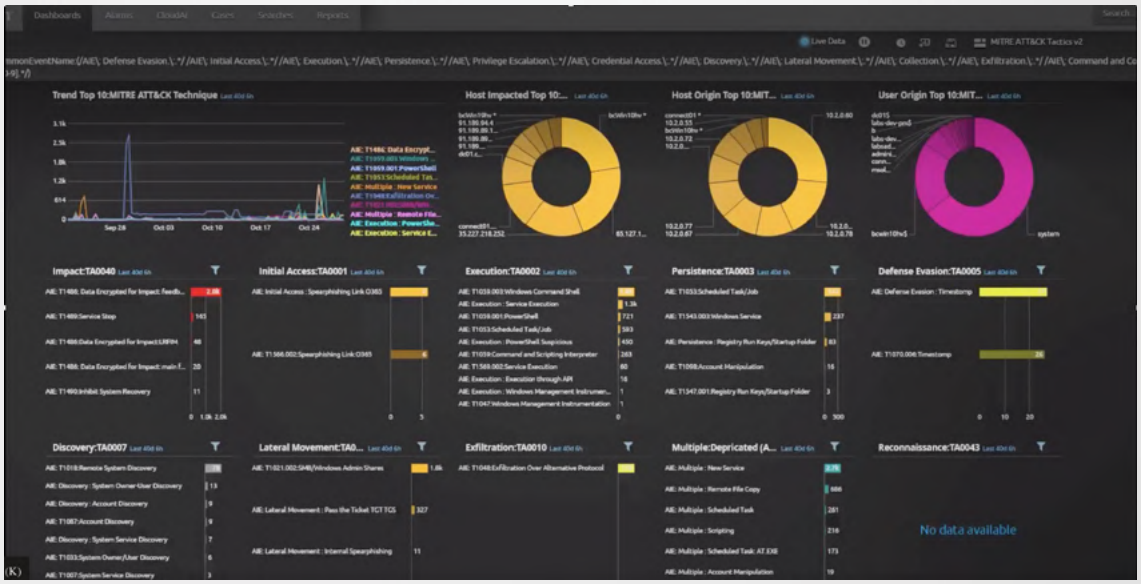


Figure 1. Activity detail for MITRE ATT&CK T1486 in the LogRhythm Dashboard.

02

T1486: Data Encrypted for Impact

This technique doesn't need a whole lot of introduction, because it is pretty much the end game of a ransomware campaign. At this stage of the ransomware is rapidly encrypting the data on your network and will soon be trying to extort a ransom.

So why focus on this technique, is it not too late by this stage?
There are two reasons for this:

1. **There's still the chance of isolating the attack**
   If you have a time analytic that can detect encryption taking place, and you can combine that with automation in your response to that detection, then you still have the possibility of isolating the damage.

2. **You can triage the infected systems for restoration and recovery**
   Identifying the attack at this stage allows you confirm the nature of the data on the systems that have been compromised and prioritize them for an efficient recovery.

Detecting T1486: Data Encrypted for Impact

https://attack.mitre.org/techniques/T1486/

When it comes to detecting T1486, MITRE gives us the following four paths to explore:

- Process Monitoring
- Kernel Driver Monitoring
- Cloud Monitoring
- File Monitoring

Process Monitoring

Process monitoring gives you a lot of visibility into adversarial activity, and it helps considerably in detection, threat hunting, and forensics. So whenever possible, you should do process monitoring on your endpoints. With this technique, MITRE specifically lists three processes you should focus on: VSS Admin; WB Admin; and BCDedit. We will touch on these later.

LogRhythm Insights—How Quickly Can You Respond?

Data from ransomware gang LockBit on their latest software claims it only takes about four and a half minutes to encrypt 100GB of files. If you think about your environment and what detections you have set up—how long would it take you to detect ransomware and accurately respond to that? Would it be four and a half minutes, would it be 40 and a half minutes, or would it be 40 hours? Understanding this allows you to define your response needs.

LogRhythm's SmartResponse™ automation enables you to launch remediation scripts in response to triggered analytics. This allows you to see if there is a ransomware attack in progress and quickly do things like shut down machines, log off users, as well as configure firewalls to try isolating any damage. Despite the fact that you have already become the victim at this point in an attack, having effective incident response in place helps to minimize the scope and impact of an attack.

Ransomware	Encryption speed	Time needed to encrypt 100GB of files	File downloading speed	Time needed to download 10GB of stolen data
LockBit 2.0	**373 MB/s**	**4m28s**	**83.46 MB/s**	**1m59s**
LockBit	**266 MB/s**	**6m16s**	**83.46 MB/s**	**1m59s**
Cuba	185 MB/s	9m	4.82 MB/s	5h45m46s
BlackMatter	185 MB/s	9m	4.82 MB/s	5h45m46s
Babuk	166 MB/s	10m	4.82 MB/s	5h45m46s
Sodinokibi	151 MB/s	11m	4.38 MB/s	6h20m31s
Ragnar	151 MB/s	11m	4.82 MB/s	5h45m46s

Unusual Kernel Driver Activity

In some cases, ransomware will load up Kernel Drivers to do encryption. For example, a recent Palo Alto Unit 42 Report[1] found that Shamoon 2 used the RawDisk Kernel Driver, which is a disc wiper, but can also, if configured with the right parameters, be used to encrypt as well.

Cloud Storage

This is becoming more and more relevant because most businesses have critical data stored in the cloud, and attackers have an increasing number of avenues to attack it. For example, Rhino Security Labs has developed a technique[2] where AWS Key Management Services can be used to get the encryption keys to attack poorly configured or poorly secured S3 buckets.

LogRhythm Insights—Keeping Tabs on Your Processes

Process monitoring is a critical part of your defense particularly with T1490: Inhibit System Recovery. If you know what processes are likely to be used by the ransomware, you can keep a close eye on what is going on across your systems.

LogRhythm allows you to quickly and easily track all the different processes being used in an attack, including volume shadow copy, as well as command lines being invoked.

Figure 2. Monitoring processes with Top Process Name widget in the LogRhythm Web Console.

[1] https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper

[2] https://rhinosecuritylabs.com/aws/s3-ransomware-part-1-attack-vector

File Monitoring

With any ransomware attack you're going to be looking at large quantities of file modifications, and this is where it's critical to focus your attention, beginning with looking at log sources. If you're a detection engineer and you're considering how to detect suspicious file activity, the first question for you to address is which log source is going to work best for you. There are many different log source types and each is going to bring its own unique vantage point. To illustrate this, let's consider three different log source types: Microsoft Sysmon, Windows Security Event Log, and LogRhythm File Integrity Monitor (FIM).

This table compares a single file-level event—a file add—and looks at what each platform brings in terms of metadata. First, as you can see, there's a lot of crossover, but there are also going to be critical gaps. For example, Microsoft Sysmon has only very recently added the user into Event ID 11, prior to that if your Detection Theory hinged on correlating user activity you wouldn't have been able to use Sysmon. Also, you'll see LogRhythm FIM, doesn't have a Process Path. So, again, if your detection hinged on processes launching from unusual places, like the user space, FIM would be a challenge in that case.

Log Sources: File Activity Metadata Comparison: File Add*

Metadata	MS Sysom (EVID 11)	MS Security (EVID 4663 AccessMask 0x2)	LR FIM
Target File Name			X (parsed)
Full Path to Target File	X	X	X
Target File Hash	*		*
Process Name	X	X	X
Process Path	X	X	
File Handle		X	
Process ID	X	X	X
User	(as of 13.30?)	X	X
Sysmon Policy	X (scoping/labeling)		
FIM Policy			X (scoping/labeling)

* Other logs from the same log source type may provide metadata missing here.

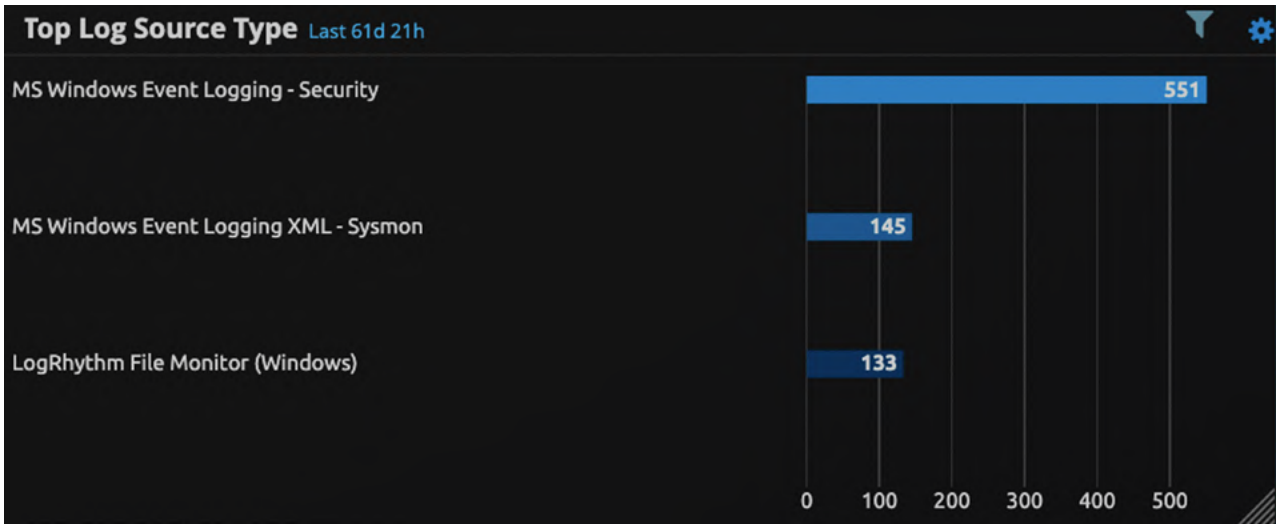


Figure 3. Monitoring log sources in the LogRhythm Web Console.

You also have to consider what activities or what file auditing activities your log source covers. In this case, there's a pretty stark difference between Microsoft Sysmon and the others. Sysmon only really has events for add and delete, whereas Windows Security Event Log and LogRhythm FIM have a much richer set of activities that they log.

Whatever source you're using it's important that you properly scope and configure the log source. File Monitoring potentially produces very high-volume log sources which can be hugely time-consuming to manage and can also produce large numbers of false positives—you're going to want to reduce these as much as possible. To drive that point home a little bit more, as far as log volume and comparing log sources is concerned, here's the comparison of those three different log source types after we ran a ransomware simulator.

Detection Theory

So now that we've considered log sources, how are we going to bring our analytics to bear for this technique? The challenge for creating a file monitoring detection theory is that different families of ransomware will interact with the file system in different ways. For example, one simulation may overwrite most of the original files with the encrypted data, another may encrypt files in a different folder and delete the original files, a third may encrypt files slowly just to try to evade detection, while a fourth will write data into a single file.

If we look specifically at REvil and Conti: REvil does an in-place encryption attack, so the encrypted documents are stored in the same sectors as the original un-encrypted document, and once that's done a random extension is added to the end of its name. While Conti opens the files for writing, and adds the encrypted key to the end of the file. Once encrypted it's overwritten back to the original file and the Conti extension is added to it.

This makes it difficult to come up with a one-size-fits-all detection theory for file monitoring. However, we can start to create a robust theory if we combine a series of three alerts: one for massive reads, one for massive writes, and one for massive deletions. If all those alerts go off together it's a pretty strong indicator that we are facing an encryption attack. But this still leaves some margin for error.

So, what does massive actually mean?

With Cryptowall, for example, the calculation was that it could encrypt up to 200 files per second, or 12,000 files per minute. So, we could we set up our detection for this, however one of the things we need to consider is what are some of the false positive considerations in this scenario? If the massive read, write, and delete activities aren't on the same set of files, especially in very large environments it could be a number of different legitimate things, such as backups, installations of software, or large-scale data moves. And so, you could potentially observe all of these things at the same time, but on unrelated sets of data.

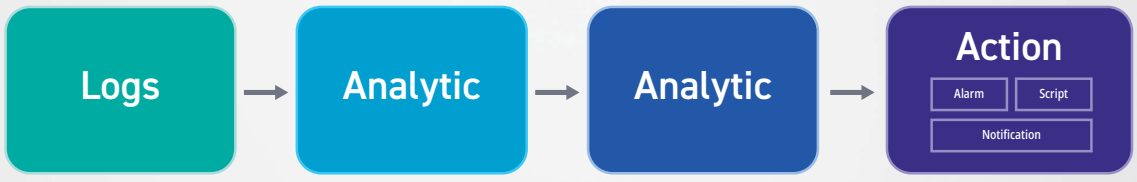
So, to tighten up our detection theory, we need to think about some things that could maybe correlate these activities better together. In the case of a ransomware attack, the files will probably reside on the same host, either a workstation or a file server. On top of this, the original files clearly have to be read, otherwise there's really no way to encrypt them. Although REvil and Conti are described as encrypting in place, lab condition detonations of the software clearly show some delete activity. Things get a little more variable with the write function as they could be on the original files, or it could be in different directories.

LogRhythm Insights—Speeding up the Log Analysis Process

Clearly, if we look at the examples above, one of the challenges with threat hunting in this way, is having access to the right logs at the right time and being able to process that data against your defined analytics. And do it quickly enough for it to be able to make a difference if a ransomware attack has been detonated.

Using LogRhythm's AI Engine you get an effective streaming analytic engine that analyzes logs in real time. It also allows you to take your analytics and feed them back into the analytic engine for a second parse. This same process can also be used to analyze activity under T1490: Inhibit System Recovery.

Advanced Intelligence Engine (AIE) Feedback Rules



03

T1490: Inhibit System Recovery

As part of an attack, adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system in order to prevent recovery. Inhibiting system recovery in this way is part of the Impact technique of the MITRE ATT&CK® matrix. The tactic comes at the very end of the kill chain and is used by ransomware to prevent the victim from recovering data or systems that have been encrypted, not having a way to get your data back besides paying the ransomware gang is obviously the end goal here.

MITRE recommends a seemingly simple detection theory for this, which revolves around monitoring the use of three often-forgotten Windows tools.

Shadow Copy

https://attack.mitre.org/techniques/T1490/

This is a service included in Microsoft Windows that creates backup copies or snapshots of computer files or volumes, even when they're in use. It's implemented through a Windows service called the Volume Shadow Copy Service (VSS VC). VSS Admin is the default Windows process that manipulates volume shadow copies of files on a given computer, these shadow copies are often used as backups, and can be used to restore or revert files back to a previous state if they're corrupted or lost. However shadow copies should not be used as the only backup solution, but they often are, especially on user workstations and as such the people responsible for ransomware campaigns often attempt to delete them so their victims can't restore file access by reverting to the shadow copies.

WB Admin

This is a Windows tool that was introduced in Vista and is used to backup and restore files, volumes, and applications. There are a number of commands that ransomware uses, such as WB Admin delete system state backup, which deletes a file that contains information about backups that's necessary for restores and is usually only deleted if the file is corrupt.

BCDedit

Boot configuration data (BCD) files provide data used to describe boot applications and boot application settings. BCDedit is the command line tool for managing BCD files. It can be used by attackers for a variety of purposes, including creating new stores, modifying existing stores, and adding boot menu options.

So, how are these used by REvil and Conti? The MITRE ATT&CK® framework lists both as using VSS Admin to delete shadow files and resize shadow storage. On top of this, some variants of REvil uses BCDEdit to force the computer to boot into safe mode when windows next restart. So, tracking activity within these systems can be powerful way of alerting to the early stages of a ransomware attack.

04

Testing Your Detections — the Benefits of Running Ransomware Simulators

As you can see from above, with REvil and Conti, there are different types of techniques that are evidenced within logs. We can analyze these in theory, but to really understand how to defend against them we need to be able to test against an active attack. Running and monitoring real ransomware takes a very locked down environment. If you are inexperienced the malware can unintentionally spread out from your test environment. This is where ransomware simulators come into their own. There are three ransomware simulators available today that can help you do that job.

Regardless of what SIEM solution you're running, or even if you have manual log collections, ransomware simulators enable you to test whether or not you can actually find and react to the types of techniques we've been discussing within your logs. You can test your prevention capabilities to see whether or not they can block this ransomware test. As you're running these simulators, you should be able to prevent their actions from encrypting the endpoint through EDR solutions or preventative hardening measures on the workstations. Of course, you can also test your incident response teams to see fast they can detect and respond to an attack.

Disclaimer: Be Wary

These ransomware simulators are owned and provided by third parties so always read the licensing agreements before using them. Also ensure they're running in an isolated test environment, even though these are simulators they do encrypt files. Although they are relatively safe, we do not recommend that you run them in a production environment.

With that said, here are three ransom simulators that are worth looking into.

Ransim

https://www.knowbe4.com/uki-ransomware-simulator-tool-ga

This is provided by KnowBe4 and is free to download from their website. It is relatively straightforward to use—just download the installer and run it. The company claims it is a 100% harmless simulation of real ransomware. It does not use any of your own files and tests 23 different types of infection scenarios. While it is easy to install and uninstall, it does lack relevant mitigation guidance. This means that if it is able to execute and encrypt files, it doesn't really tell you how to prevent that in the future. But it's something that definitely could help you understand how to harden your environment.

Shinolocker

https://shinolocker.com/

This is a really cool ransomware simulator, although it hasn't been updated for a while. It's also easy to install, run, and uninstall, and provides a web interface. One of the down sides, however, is that you need to reduce your security settings to use it as most antivirus technologies will detect it.

Mauri870

https://github.com/mauri870/ransomware

If you want to run a full end-to-end ransomware attack, Mauri870 will provide the best experience. It runs in the background and encrypts files in AES 256 and is multi-threaded. So, it's really fast. There's also an option for TOR Proxy Support. You can even chain this together with something like Metasploit to test your detection system across all the different stages of a typical attack, from phishing email delivery to detonation. To sum up it provides the best scenario of how ransomware works and can be used in end-to-end tests. However, it does require that you know how to set the test environment.

05

Making the Most of MITRE to Fend Off Ransomware

In an ideal world you'll be detecting and blocking attacks as early as possible in the kill chain. Figures vary on how long the average ransomware sits on a network — anywhere between five and 45 days — before encryption starts. That's a long time to be able to find it and kill it. However, the reality is that attacks get under the radar and pervasively move into an organization's network, so it's critical that you can also spot and respond to ransomware attacks as they happen, even once they have been detonated.

If you can search for and detect the techniques listed in the MITRE ATT&CK® Framework, then you stand a good chance of not only having a deeper understanding of what normal activity looks like in your environment, but also knowing when something strange is happening, including being able to detect lateral movements, abuse of privileged accounts, and suspicious process executions.

By building detections based on the TTP details from MITRE ATT&CK® within your own monitoring or detection & response platform, you will be able to detect the documented techniques, as well as activity that is suspicious and could lead to malicious activity sooner rather than later. Ransomware is a dangerous foe; making certain you have an ability to identify malicious activity as early on in an attack as is possible will help lower the risk of successful attack and the resulting negative impacts on your organization.

06

Conclusion

MITRE ATT&CK® is a powerful way to classify and study adversary techniques and understand their intent. ATT&CK can be used many different ways to improve cybersecurity efforts. This paper has focused on how you can use ATT&CK to enhance, analyze, and test your threat detection efforts. The LogRhythm Labs team is dedicated to building ATT&CK into the LogRhythm NextGen SIEM Platform to ensure comprehensive, up-to-date, and verifiable threat detection.

About the Authors

Randy Franklin Smith

Randy Franklin Smith is an internationally recognized expert on the security and control of Windows and AD security. Randy publishes 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.

Brian Coulson

As Threat Research Senior Engineer for LogRhythm Labs, Brian Coulson works to keep abreast of current cyberthreats and news, develop threat detection and response content, and demonstrate how the LogRhythm NextGen SIEM Platform detects and responds to threats. In this role, he engages with the LogRhythm Community and offers advice and solutions to remediate security-related issues. Prior to LogRhythm, Brian was a lead information security engineer for a LogRhythm customer.

Dan Kaiser

As a Threat Research Engineer for LogRhythm Labs, Dan Kaiser develops content for the security-focused modules in the LogRhythm Knowledge Base, such as UEBA, NDR, and CIS Controls. Before LogRhythm, Dan worked as a network engineering manager for an oil and gas company and as an IT director at a law firm. He also worked as an engineer at a Citrix Metaframe-based application service provider.

Sally Vincent

Sally works as a Threat Research Engineer for LogRhythm Labs. She has broad experience in systems administration and working with various industries including, financial, healthcare, government, retail, MSSP, from SMB to Enterprise size.

About LogRhythm

LogRhythm helps busy and lean security operations teams save the day—day after day. There's a lot riding on the shoulders of security professionals—the reputation and success of their company, the safety of citizens and organizations across the globe, the security of critical resources—the weight of protecting the world.

LogRhythm helps lighten this load. The company is on the frontlines defending against many of the world's most significant cyberattacks and empowers security teams to navigate an ever-changing threat landscape with confidence. As allies in the fight, LogRhythm combines a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help SOC teams close the gaps.

Together, LogRhythm is ready to defend.
Learn more at logrhythm.com.

www.logrhythm.com // info@logrhythm.com

United States: 1.866.384.0713 // United Kingdom: +44 (0)1628 918 330
Singapore: +65 6222 8110 // Austrailia: +61 2 8019 7185