WHITEPAPER

MyCyberIQ™
STAY AWARE. STAY SMART. STAY SECURE.

Security

Ransomware Technical Whitepaper

www.mycyberiq.io

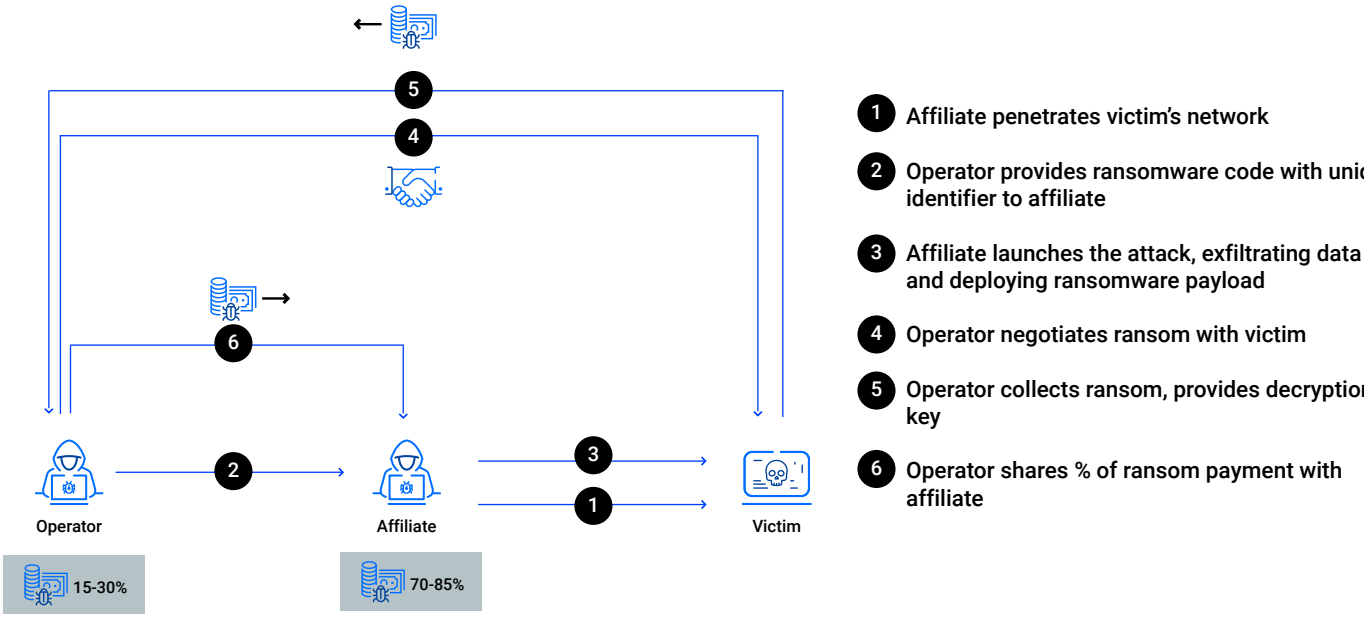
Contents

Ransomware-as-a-Service (Ransomware 2.0)

The cybercrime ecosystem is driven by the same economic forces as regular markets. A new business concept or idea can quickly become the new standard, eventually replacing previous business practices.

One of these revolutions happened in the underground with the introduction of the profit-sharing Ransomware-as-a-Service (RaaS) model. In this model, ransomware operators work with affiliates, but it is not a simple subscription model as often described. Today, you are more likely to be hit by one of these RaaS groups than by the older ransomware models.

Ransomware operators develop the malware and run the infrastructure. Affiliates, resembling self-employed contractors, are experts in compromising networks. After successful breach and deployment, ransomware operators negotiate and collect the ransom and distribute their shares to the affiliates. If this reminds you of a heist movie, you are correct. A group of skilled experts that gets together to do a special job and escape with a large sum of money. Using affiliates, ransomware groups run operations at scale, attacking multiple organizations simultaneously, each successful attack further improving funding, tooling, and best practices.



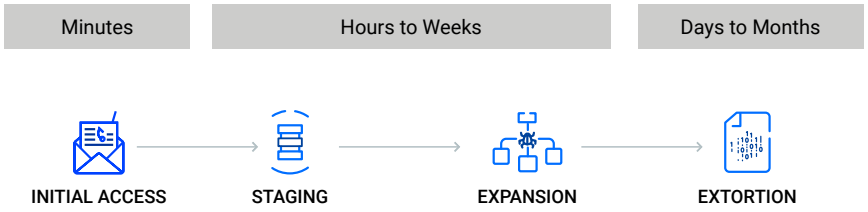
Ransomware-as-a-Service profit-sharing model. Affiliates own access to networks and receive the biggest share of profit.

This new model motivates threat actors to find new ways to maximize the potential yield. Attackers are more business savvy, reinvesting profits to advance tactics and tools for the next attack. With a better understanding of the impact on the business, pressure can be increased, and ransom demand can be more precisely calculated. This new model was adapted across all verticals and company sizes.

Less known is the revenue sharing ratio – it heavily favors affiliates, who often get up to 80% or 90% of payment. While ransomware operators lead negotiations and get all the media credit for successful attacks, affiliates get the largest share of profit. In the last few years, the power has shifted from those who control the ransomware code to those who control access to networks.

Anatomy of the ransomware attack

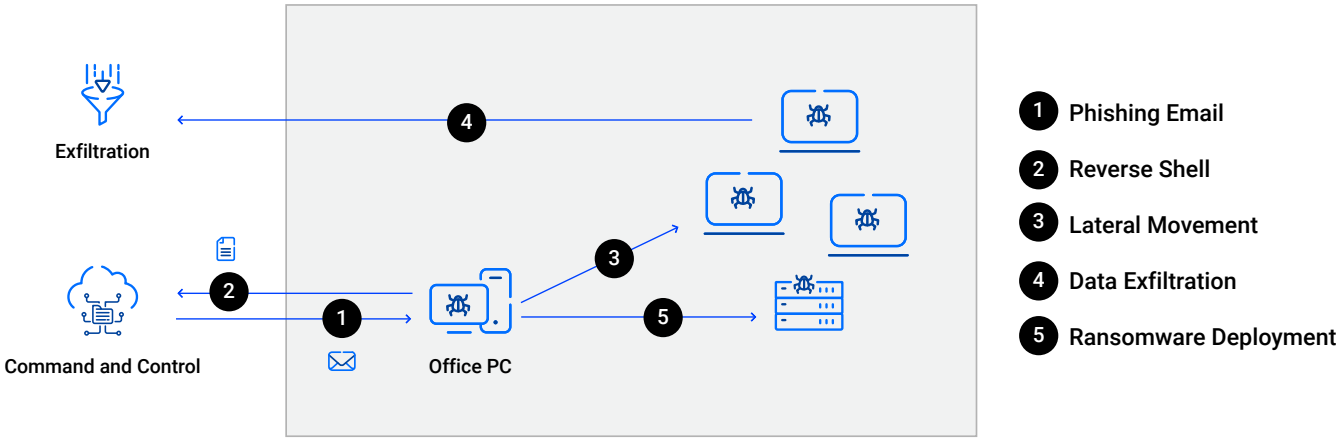
This shift of power changed the anatomy of ransomware attacks. Previously, attacks were often opportunistic and utilized worm-like behavior (WannaCry), focusing on the most direct route to monetization of attack. In the profit-sharing model, threat actors adopted tactics, techniques, and procedures from advanced persistent threat (APT) groups. The focus is on maximizing damage and pressure, not on the speed of attack. Attackers can spend weeks or months preparing for the execution of an attack.



Ransomware deployment is often preceded by weeks of preparations.

As a result, modern ransomware is just another type of payload, deployed at the final stage of the kill chain after extensive preparation. Defense-in-depth architecture is a proven strategy, and the best protection is still provided by high-quality prevention security control, enhanced with great detection and response with a focus on fast response and minimizing false positives.

The following diagram illustrates the anatomy of a typical ransomware attack. A user receives a phishing email, after opening it, the machine is infected **(Initial Access)**. Reverse shell to a command-and-control server **(C&C)** is established **(Staging)**. Ransomware affiliates run reconnaissance, identifying, and compromising systems **(Expansion)**. Finally, after data is exfiltrated, ransomware is deployed, and the victim is contacted by the ransomware operator **(Extortion)**.



Anatomy of a typical ransomware attack. Double extortion is a new standard, preceding the ransomware deployment.

Let's look at the different parts of the modern ransomware kill chain.

Initial Access | Staging | Expansion | Extortion

The initial infection vector often depends on the size and security maturity of the target. Generally, automated scalable attacks are used for smaller companies, while corporations are targeted by spear-phishing campaigns. The effort that threat actors invest into the attack is proportionate to potential earnings.

For larger corporations with mature security controls and processes, phishing and social engineering remain the primary infection vector. Another infection vector is supply-chain attacks – for lucrative targets, it is easier to focus on the vulnerable periphery

instead of attacking the well-protected front gate. Small and medium-sized companies can be targeted by sophisticated threat actors as part of a larger operation.

For small and medium companies, insufficient protection of remote access is one of the most common attack vectors. This typically means access via RDP, using stolen or guessed credentials. Another common initial vector is unpatched internet-facing systems. Attackers are targeting 3rd party systems with known vulnerabilities, such as VPN and remote access solutions. Strong authentication plays a critical role in ransomware risk mitigation.

After gaining initial access, threat actors need to prepare a staging environment for the attack. There are typically two goals for this stage – escalate privileges and establish persistency, all while avoiding detection. Privilege escalation often involves the use of exploits or penetration tools like Mimikatz or Cobalt Strike.

For some threat actors, establishing persistent access is the final goal. Access brokers can sell this access on dark web marketplaces to other threat actors, such as affiliates associated with one of the ransomware groups.

The expansion involves more reconnaissance and lateral movement across the network. While tools like BloodHound can be used at this stage, professional attackers try to maintain a low profile by using tools and commands that are native to the environment. This is often referred to as “Living off the Land” (LOL) and includes the use of tools like WMIC or PowerShell. Another common practice is to identify tools that are used by system administrators – for example, PsExec or popular remote-control software like TeamViewer or AnyDesk.

Therefore at this stage, threat actors can often be detected only by their behavior and not by the malicious tools they are using.

To reach these astronomical ransoms (compared to an average ransom just a few years prior), threat actors are focused on maximizing the pressure on their victims. Simple encryption of random data is no longer enough – double or triple extortion is becoming standard practice. A ransomware attack can be combined with data exfiltration (for blackmailing purposes), denial of service attacks, or harassment of executives, partners, and customers. A better understanding of business and corporate financials is playing an important role during the extortion phase – threat actors often understand the impact of their actions, know which information is valuable, are familiar with incident response procedures, and understand your cyber insurance coverage.

Before a ransomware payload is delivered, threat actors locate and destroy all available backups. The actual ransomware payload can be delivered using a wide variety of methods, but deployment usually relies on common, simple, and reliable tools, such as PsExec/WMIC, Group Policy, or even management tools such as Microsoft System Center Configuration Manager.

How to defend against modern ransomware attacks

The best protection against modern ransomware attacks is to implement a defense-in-depth architecture. Start with reducing the attack surface, combined with automated prevention controls to prevent the vast majority of the security incidents. For the remaining incidents, you must rely on security operations, enhanced with great detection and response tools.

Reducing Attack Surface

The best cyberattack is the one that never happened – and one of the best ways to prevent attacks is to implement and follow a set of cyber security best practices. Reducing your attack surface is one of the most cost-effective ways to improve your cyber resilience – through reliable asset management, automated patching, implementing zero-trust architecture, and identifying and mitigating misconfigurations and insecure default configurations.

Automated, scalable attacks typically start with scanners identifying vulnerable systems on the internet, benefiting from inconsistent or slow patch management processes. With the wide adoption of remote work programs, continuous patching of all systems can prevent attackers from gaining access through periphery systems. **Patch Management** is an automated module to help keep operating systems and software applications up to date and includes reporting for full visibility and control over the status of missing/failed patches across all endpoints.

When attackers fail to identify vulnerabilities in your software stack, they focus on vulnerabilities in your security policies and implementation. **Endpoint Risk Analytics** provides critical insights about endpoints' misconfigurations and application vulnerabilities. This includes recommendations for endpoints (like OS hardening or policy configurations), but also user-related risks, such as high malware detection count for a specific user. Recommendations are rated by severity, and fixes can be either deployed automatically, or required manual steps are provided.

Both patch management and risk analysis provide maximum protection only when implemented as continuous processes. Choosing a well-integrated, easy-to-use solution helps establish good cyber hygiene routines across your organization.

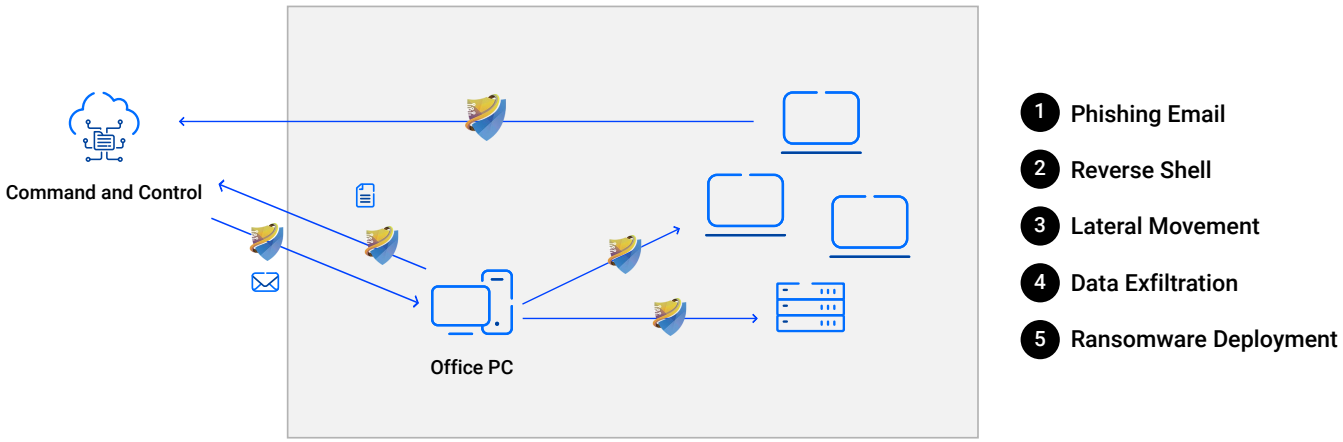
Multilayered Protection

While improvements in attack surface management are very good at stopping opportunistic threat actors, they are unlikely to stop targeted or persistent attacks. A determined attacker will find other ways in and leverage a wider array of techniques, such as social engineering and supply-chain style attacks.

A defense-in-depth architecture is a proven approach to take care of the fallout. The foundation of your protection should be a set of high-quality prevention security controls, providing wide coverage and applying different techniques to recognize malicious intent.

Each part of the security stack needs to be balanced – detecting the threats without generating too much noise in the form of false alarms. MyCyberIQ's partners has spent over 20 years fine-tuning our algorithms to provide this balance.

During each stage of the attack, threat actors must bypass multiple security checks – it is common for a single malware to trigger multiple detections. To show this on an example, let's look at the initial access established through the phishing email.

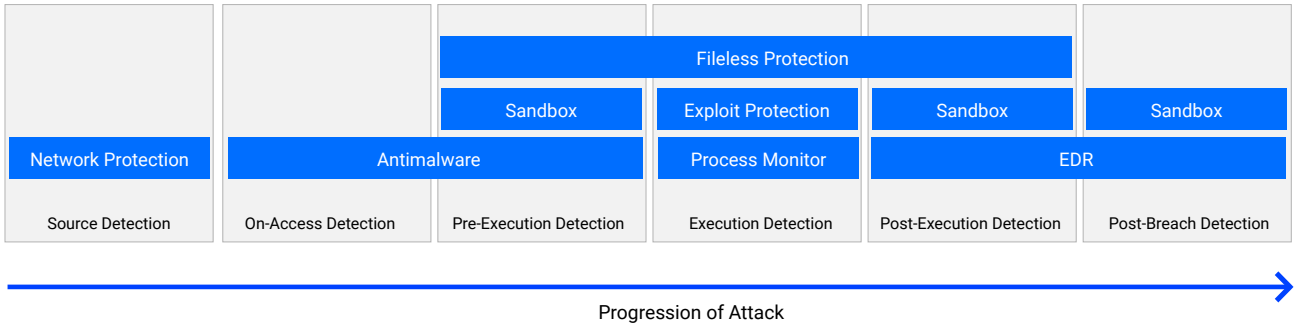


Example of automated MyCyberIQ detections during the first step of the ransomware kill chain.

This simple attack triggers multiple detections in the Business Security platform.

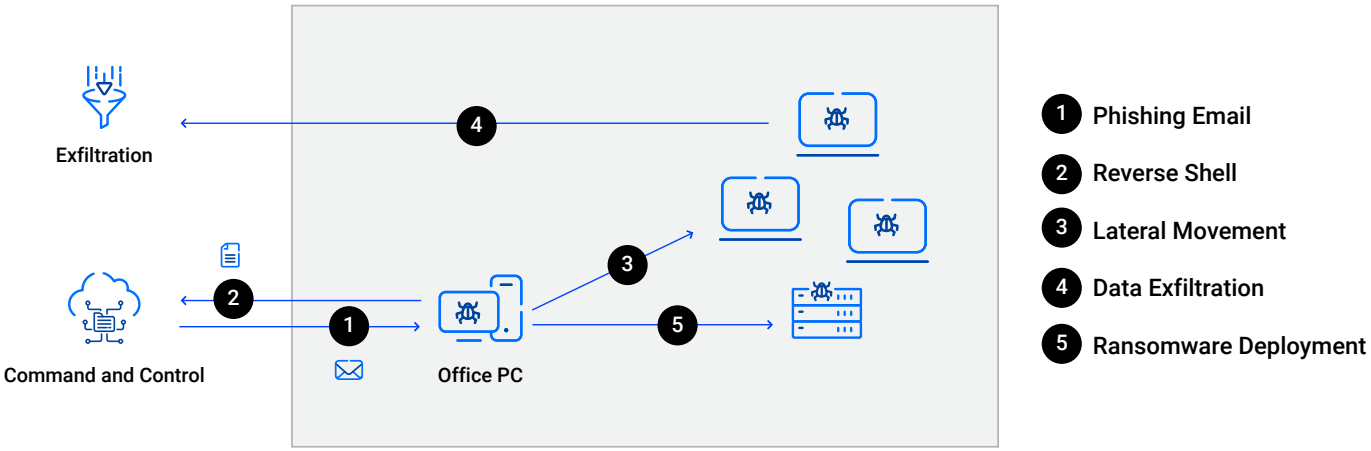
1. Before an email with a malicious attachment arrives in the mailbox, **Security for Email** uses multiple scanning engines to detect threats, combined with advanced threat intelligence.
2. If an attachment is opened, a static anti-malware engine scans if it is a known threat, offering the best performance when detecting previously known threats. If the static analysis doesn't recognize this file, our **tunable machine learning** provides customizable detection of sophisticated threats, including support for obfuscated scripts and various archive formats.
3. After a document is opened, but before the embedded macro can be executed, a document is uploaded to the **Sandbox Analyzer.** The solution detonates the sample in an isolated environment, providing an in-depth analysis of its behavior to better understand the functionality of the Visual Basic for Applications (VBA) code.
4. If VBA code is executed in memory, various security controls are activated. First, **Fileless Attack Defense** is triggered. This includes analysis of the code being executed, but also runtime protection using the Antimalware Scan Interface (AMSI), code injection detection, and scanning process memory after unpacking. **Exploit Defense** is designed to provide special detection for the most popular software, including Microsoft Office. Finally, **Process Inspector** provides behavior-based real-time monitoring of processes, which would be triggered if a suspicious child process is launched – for example, if the Microsoft Office executable tried to create a new command prompt process.
5. The malicious VBA macro starts an attack by downloading more code from the C&C server. However, before the file download is even started, **Network Attack Defense** uses advanced threat intelligence for IP and URL reputation scanning data to establish If the C&C server address is recognized as malicious, blocking the file download. If the file download is allowed, execution of the file triggers the whole chain of security controls again.
6. The malicious code does execute, opening a reverse shell for the attacker. Launching a reverse shell would trigger all the previous detections again, including IP/URL reputation, additionally, Network Attack Defense would recognize the traffic pattern as a reverse shell connection and block it.

This was an example of overlapping security modules for one of the stages of an attack, but the same security stack would be used for the other parts of a ransomware attack – from privilege escalation to lateral movement across the network. Each of these detections can trigger an incident response, preventing a ransomware attack from fully expanding. MyCyberIQ security stack provides protection before, during, and after a suspicious event.



Multi-layered security mapped to different stages of malware execution.

While each of these security controls is a powerful tool, it's the combination of them that results in the top ranking of **MyCyberIQ** in independent efficacy tests. The well-integrated solution brings all these security controls together, and central correlation engine is continuously analyzing data collected from different sources. Even when threat actors perform an action that is typically not malicious, it can trigger an incident based on the context of previous actions – for example, when a PowerShell script is trying to upload some data after lateral movement was detected.



Multiple stages of ransomware deployment can trigger incident detection. Modern ransomware attacks generate enough noise to be detected by security teams.

Minimizing dwell time of threat actors

Relying on backups, supplemented with prevention, was an ineffective security strategy even when dealing with the previous generation of opportunistic ransomware attacks. With the modern ransomware threats focused on maximizing damage and pressure on victims, this approach is obsolete.

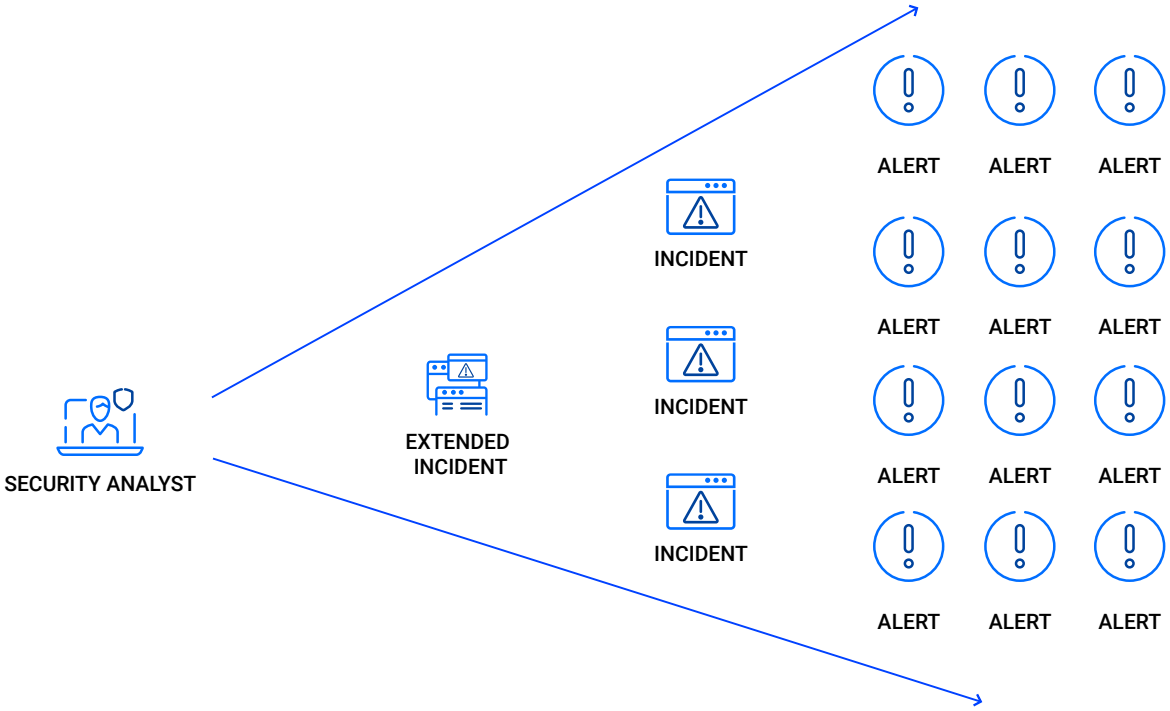
But there is a silver lining – threat actors that adapted techniques from state-sponsored APT groups need more time with hands-on hacking and preparations for the final stage of an attack, generating noise and leaving behind clues that can be detected and recognized by security teams. The best approach to counter these new tactics is to adapt defensive tools that are effective against APT groups.

This is easier said than done. Many small and medium businesses don't have mature security operations, and lack of qualified resources is affecting companies of all sizes. Lack of operations preparedness is one of the main reasons why new ransomware tactics are so effective.

For many customers, managed services, such as Managed Detection and Response (MDR) are the right option to complement their security stack and eliminate the operational overhead of running a security operations center. MyCyberIQ

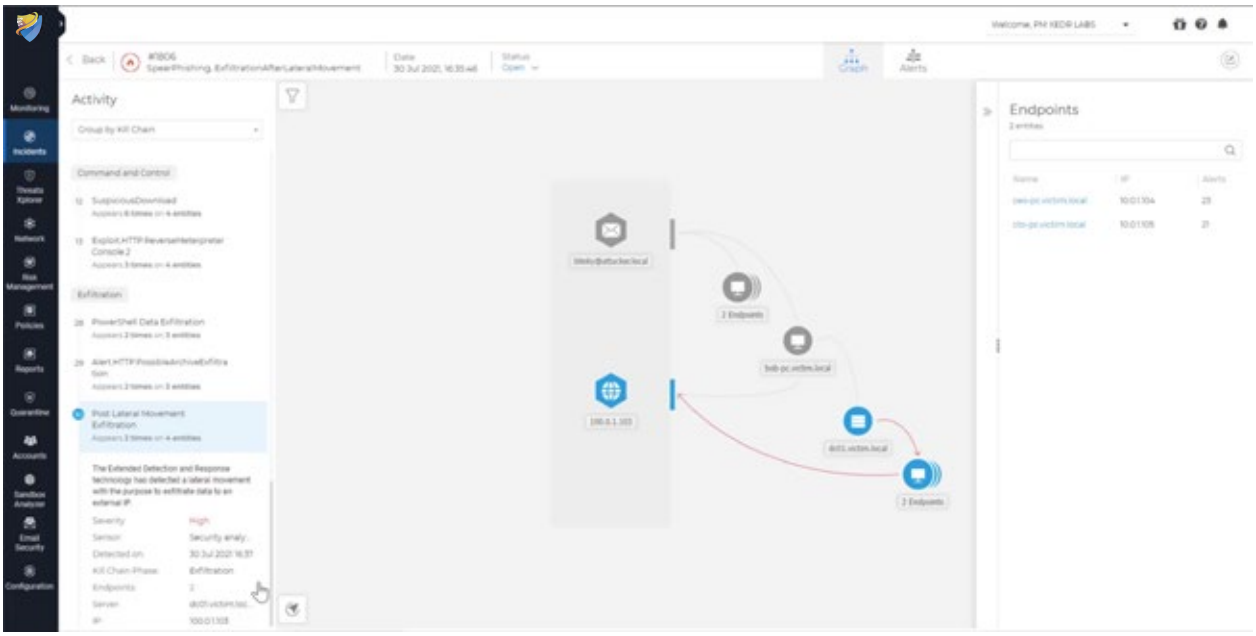
MDR Threat Hunting provides a comprehensive approach to reducing compromise of business systems and attacker dwell-time. Continuous and proactive assessment of risks to your business, combined with a deep understanding of your networks and systems activity, enables us to recognize any abnormalities. MyCyberIQ MDR also continuously monitors the dark web to discover customer or brand information, including customer credentials, intellectual property, holdings and subsidiaries, and other customer-specific information.

Other customers prefer a more hands-on approach and add Endpoint Detection and Response (EDR) solution to their security stack. It is integrated with prevention controls into a single-agent, single-console solution. **MyCyberIQ** EDR is designed to minimize the time threat actors can stay undetected after the initial intrusion. To achieve this goal, EDR is looking for signs of malicious behavior. It uses endpoints as sensors, analyzing processes, files, registry keys, scripts, and much more. Events are collected by agents, then analyzed for suspicious behavior and assigned a risk score. If the probability of malicious intent is high enough – a security incident is reported. In addition to analyzing individual incidents, security analytics also analyze relationships between individual alerts and incidents. With cross-endpoint correlation, a security incident can be detected faster, and we can interrupt the kill chain before it fully develops.



With extended EDR, we can provide high-fidelity incidents early in the attack kill chain

An EDR solution doesn't see all alerts as equal – it assigns them different weights and treats them differently. For example, automated blocking of malware in an email attachment is an isolated incident that doesn't require human intervention. On the other hand, detecting a ZeroLogon attack against one of the domain controllers from inside the network should trigger an immediate response. Cross-endpoint correlation can use this incident to map the whole kill chain, even triggering detections that would otherwise go unnoticed – for example, a seemingly harmless PowerShell script is blocked if it is linked to previous actions of threat actors (PowerShell exfiltration after lateral movement).

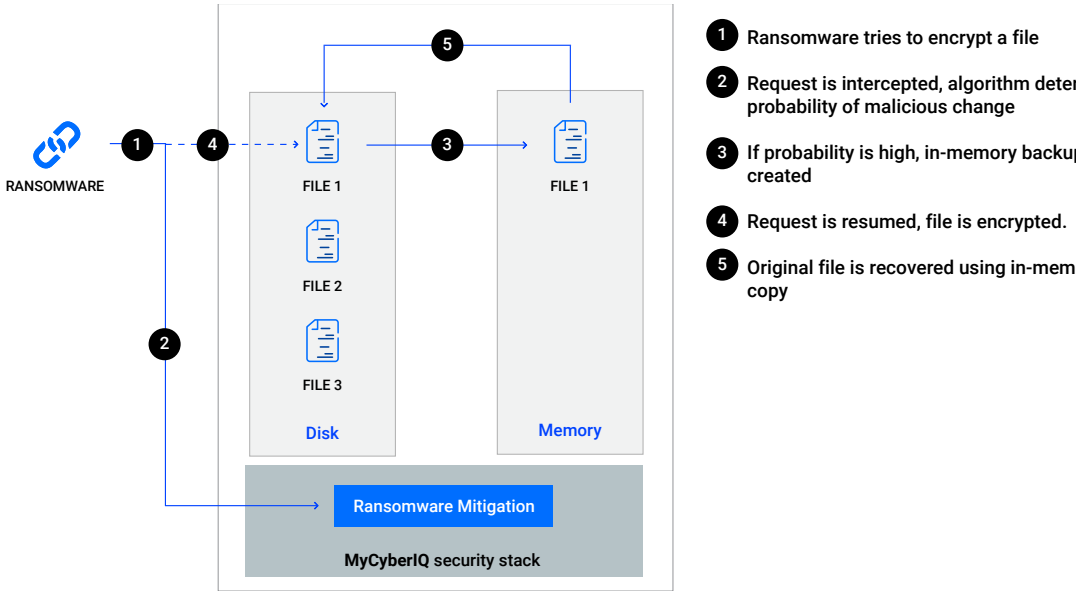


Example of extended incident visualization. PowerShell data exfiltration after the lateral movement was automatically detected.

Ransomware Mitigation

One of the most important aspects when designing defense-in-depth architecture is to assume that threat actors can always bypass the security controls in place. For example, threat actors can locate an unmanaged machine to launch a ransomware attack.

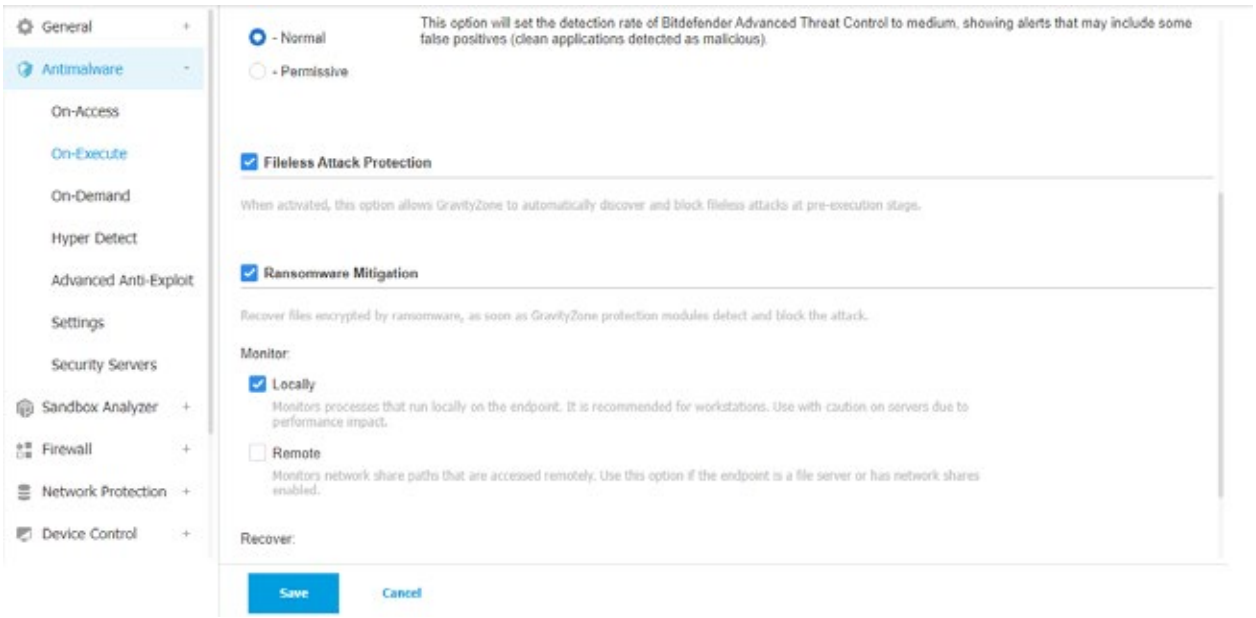
Ransomware Mitigation is a feature designed to mitigate the impact of an active ransomware attack. When a file is encrypted the randomness (or entropy) of the file goes up significantly. Ransomware Mitigation monitors for this increase in entropy of files on the disk, and during write attempts. When a request is made to encrypt a file (an increase of randomness over a certain limit), a temporary backup is created in memory and the original file is restored after the file changes are done. Importantly this method does not rely on the Volume Shadow Copy service or other static backup solutions, as this backup data is almost always deleted by threat actors. Requests to delete shadow copies are one of the triggers for an EDR incident. Using this approach, we provide ransomware mitigation even against previously unseen ransomware variants.



Ransomware Mitigation recovers the content of encrypted files using an in-memory backup

Ransomware Mitigation is supported for both local and remote scenarios. For Local Ransomware Mitigation, administrators can configure MyCyberIQ's security policy to monitor endpoint processes and recover the encrypted files as soon as the adaptive technology detects and blocks the attack. Even if ransomware manages to encrypt the local files, mitigation technology immediately jumps in to recover those files, either automatically or on-demand where the admin controls the timing of the recovery of the encrypted files.

For Remote Ransomware Mitigation, the security administrator can enable the technology to monitor network share paths that can be accessed remotely and prevent the files from being encrypted. On the remote endpoint, the user agent confirms that Ransomware Mitigation intercepted the remote malicious process behavior and protected the files. **MyCyberIQ** administrators can quickly run audit reports and find out more information about the IP address from where the remote ransomware attack was launched and the security module which protected the endpoint, and they can also receive an email notification when an attack is blocked containing information about the attacker's IP address.



Ransomware Mitigation can mitigate attacks against local and remote files

Business Security platform also offers ransomware activity reporting for a quick overview of infected machines and their restore status. After an active attack is detected, you can quickly understand how it impacted your endpoints and the steps that are needed to recover your business.

Conclusion

To summarize, cybersecurity is a game of cat and mouse, with both sides constantly innovating and improving tools and techniques. A reliable, world-class prevention was always critical in stopping threat actors. But with the modern Ransomware-as-a-Service profit-sharing groups and state-sponsored threat actors, innovation is now focused on detection and response capabilities. Security incidents will happen. But security breaches are avoidable with proper security hygiene, solid defense-in-depth strategy, and great security tools. Combine this technology foundation with mature security operations (in-house or through managed services) for greater efficiency and cyber resilience.