COMODO

Ransomware Lessons from REvil’s Return

Five Vital Steps to Protect Your Company Against a Ransomware Attack

200 Broadacres Dr,
Bloomfield, NJ 07003

Tel: +1 (888) 551-1531
Tel: +1 (973) 859-4000

www.comodo.com
platform.comodo.com

A little over a year after the SolarWinds attacks exposed a giant backdoor into the networks of major organizations and government agencies, REvil launched a similar attack. The Kaseya IT management software suffered a similar supply chain-style attack. A patch, corrupted with ransomware, was served out to thousands of customers disguised as a legitimate update.

Unlike other ransomware attacks originating from emails, direct attacks, or files downloaded from the web, this attack took root because the malicious patch came from a trusted source and was allowed to execute without being scanned.

After the SolarWinds and Kaseya attacks, the question remains: How can organizations manage to protect themselves without wasting large amounts of time and resources conducting an in-depth review of every file they download? This article will explore the current challenges with ransomware and how companies can manage this problem.

Dark Does Not Mean Done For

The Kaseya attacks came from the REvil group, known for previous ransomware attacks, with a history of demanding large multi-million dollar ransoms.

Then shortly after the Kaseya attacks took place, the REvil group mysteriously disappeared from the internet. The sites that businesses used to pay ransom and acquire decryption keys were suddenly offline. There are theories that the sites came down due to nation-state-level actions. However, it might be that the group received too much attention for this attack and stepped their operation back into the shadows while things cooled off.

After only a few short months of being gone, the REvil servers re-appeared on the internet, and while the group was silent, people were quick to breathe a sigh of relief. This proved to be a mistake as the disappearance was only temporary. New ransomware tied to the group is now being cataloged and is infecting new machines. While it is still unknown why they disappeared in the first place, there is no doubt they are back in business.

The Ransomware Machine Never Stops

It’s a mistake to believe that just because a high-profile group like REvil isn't making attacks that organizations are safe from ransomware. There are plenty of other groups out there producing malware at a rate of 560,000 new instances per day. Ransomware is hugely profitable, with average ransom demands rising to $5.3 million in 2021. These profits allow bad actors to pay for programmers to develop new and evolved strains through profits from previous attacks.

A Five Step Defense

Defending against these attacks is not hard and can be summarized in 5 easy steps. These steps cover best practices that should be in most organizations but in many cases are not. Following this guide and implementing these practices will help mature your organizational security model and significantly increase your protection against ransomware.

Step 1: Preparation - This is the Way

Businesses can't stand by idly and hope that they won't be a target. They need to be proactive in protecting their assets. It is not a matter of "IF" they are a target; only "WHEN" the attack will hit. A ransomware attack occurs every 11 seconds. The steps businesses take to prepare for an attack and minimize the impact will determine the scope of the damage they suffer and the time needed for recovery.

Part of preparation is knowing the steps that will be taken when an attack happens. In the chaos of an attack, it is easy for actions to be missed or people to be left standing around lost. An incident response plan outlines exactly what will be done and who is responsible for carrying it out. Having an orderly incident response plan eliminates the guesswork and provides everyone with a purpose.

To generate an incident response plan, you need to understand the critical software and infrastructure powering your organization. Knowing this will help your organization establish if there are sufficient controls in place to protect the data on these systems and the capacity to restore them to operations quickly. This dramatically speeds up the recovery time post-attack.

Step 2: Anti-Virus - Your First Line of Defense

The easiest way for businesses to control the malware epidemic is to ensure that they have a modern antivirus (AV) installed and updated. Not every attempted attack will use advanced malware. Many utilize old variants that have been around for years. Traditional signature-based AV solutions are fully capable of catching and stopping these strains.

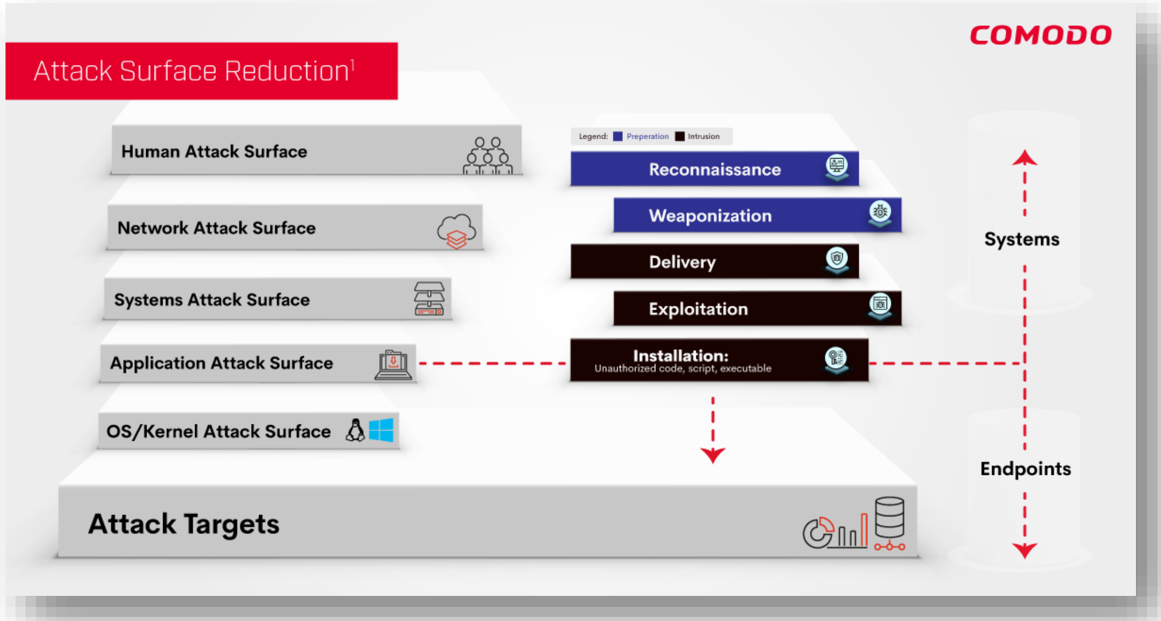
Many modern AV solutions also use behavioral data to help determine whether the software is malicious to go above and beyond this. Behavioral information helps identify new strains or altered old strains that don't match previous signatures. AV solutions use this information to catch many types of ransomware before they get a foothold in your organization.

Step 3: Harden Your Infrastructure

Part of protecting your business involves setting up and maintaining operational best practices. Hardening security throughout the organization, including up-to-date patch management and a vulnerability remediation program, helps block easy holes that attackers exploit. Attackers often use existing software and infrastructure vulnerabilities to execute malicious programs and kick off ransomware attacks. By maintaining a vulnerability scanning and management program in conjunction with keeping patches current, security teams can catch and close these holes before bad actors exploit them.

Organizations need to evolve their security posture to ensure that all components are included in hardening. It is easy to overlook IoT (internet of things) devices, network devices, network services, and facilities. These items are all interconnected on the network and can serve as easy targets for attackers. Without adequate hardening, these devices can easily serve as a pivot point for cybercriminals to move deeper into your network.

Another best practice that makes infrastructure more challenging to attack is adhering to least privilege for critical assets. Least privilege ensures that no single individual has access to everything. This will reduce the potential impact when a bad actor gets their hands on compromised credentials.



Step 4: Back-Ups Are Your Best Friend

Backups can be your salvation if the worst occurs. Rather than paying the ransom, organizations with current good backups can instead purge the infected machines and rebuild them to a safe state. This plan, though, requires regular and frequent backups of mission-critical data throughout the organization. So even end-user desktops should have mission-critical content backed up to a central location.

The downside of backups is that they aren't always faster than paying a ransom and unlocking systems with the key. But the advantage is not paying out a ransom and funding the bad guys to attack again in the future.

Step 5: Consider Cutting Edge Defenses

Threat actors have evolved, but so has malware protection. Cutting-edge technology in prevention is vital to staying ahead of new and evolving malware. New technologies such as Kernel API virtualization ensures that untrusted software never accesses the underlying OS. So when a new piece of software takes dangerous actions, it is safely segmented off.

Other powerful tools such as AI and ML help assess how programs behave and identify questionable behavior before allowing it to launch. This behavioral analysis collects state-specific behavior, such as whether the launching programs are trusted. It can also assess the age of file signatures to determine if what usually would be a trusted file might have been overwritten, even if the signature is legitimate.

Technologies like these working together can catch attacks such as Kaseya and prevent them even when they have not been seen before or originate from what would have been a trusted program.

More Than An Ounce of Prevention

Just because bad actors are still pushing ransomware out en masse does not mean businesses need to cower in fear of waiting to be hit. Instead, organizations can take steps to address the problem before it strikes proactively. Simple steps such as up-to-date AV and patch management go a long way toward preventing many attacks. Organizations that want to be a step ahead of the next Kaseya-style threats can leverage cutting-edge technologies to identify malware by its behavior and take steps to isolate it before it can get its tendrils into your assets.

Comodo Advanced Endpoint Protection can help your organization take control of protecting its endpoints. Using a Zero Trust Architecture, Comodo provides cutting-edge protection against new and evolving threats. Comodo provides a depth of visibility across your IT ecosystem to discover attacks early and provide alerts so you can quickly take action. Schedule a demo to learn more about how Comodo's Advanced Endpoint Protection can help protect your enterprise.

COMODO

ABOUT COMODO CYBERSECURITY

In a world where preventing all cyber-attacks is impossible, Comodo provides active breach protection with its cloud delivered, Zero Trust platform. The Comodo Dragon platform provides a Zero Trust security environment that verdicts 100 percent of unknown files. The platform renders an almost immediate verdict on the status of any unknown files, so it can be handled accordingly by software or human analysts. This shift from reactive to proactive is what makes Comodo unique and gives them the capacity to protect your business—from network to the web to cloud—with confidence and efficacy.

Comodo has experts and analysts in 185 countries, protecting 100 million endpoints and serving 200,000 customers globally. Based in Bloomfield, N.J., Comodo has a 20-year history of protecting the most sensitive data for businesses and consumers worldwide.

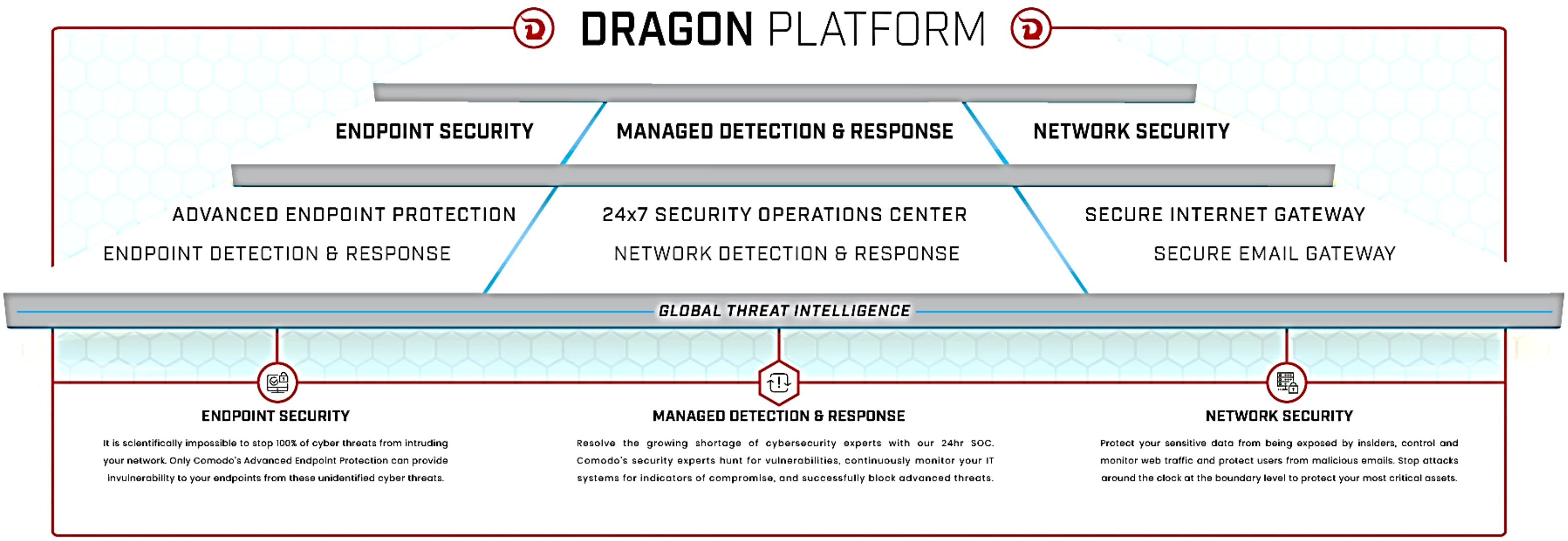
ACTIVE BREACH PROTECTION FOR YOUR BUSINESS

Comodo provides Active Breach Protection in a single platform. No one can stop 100% of threats from entering their network so Comodo takes a different approach to prevent breaches.

Experienced intrusion? Contact us at 1 (888) 551-1531
Visit comodo.com for your free 30-day trial

ZERO TRUST ARCHITECTURE

THE LEADING CLOUD-NATIVE CYBERSECURITY PLATFORM



DRAGON PLATFORM

ENDPOINT SECURITY
MANAGED DETECTION & RESPONSE
NETWORK SECURITY

ADVANCED ENDPOINT PROTECTION
ENDPOINT DETECTION & RESPONSE

24x7 SECURITY OPERATIONS CENTER
NETWORK DETECTION & RESPONSE

SECURE INTERNET GATEWAY
SECURE EMAIL GATEWAY

GLOBAL THREAT INTELLIGENCE

ENDPOINT SECURITY

It is scientifically impossible to stop 100% of cyber threats from intruding your network. Only Comodo's Advanced Endpoint Protection can provide invulnerability to your endpoints from these unidentified cyber threats.

MANAGED DETECTION & RESPONSE

Resolve the growing shortage of cybersecurity experts with our 24hr SOC. Comodo's security experts hunt for vulnerabilities, continuously monitor your IT systems for indicators of compromise, and successfully block advanced threats.

NETWORK SECURITY

Protect your sensitive data from being exposed by insiders, control and monitor web traffic and protect users from malicious emails. Stop attacks around the clock at the boundary level to protect your most critical assets.

200 Broadacres Dr,
Bloomfield, NJ 07003

Tel: +1 (888) 551-1531
Tel: +1 (973) 859-4000

www.comodo.com
platform.comodo.com