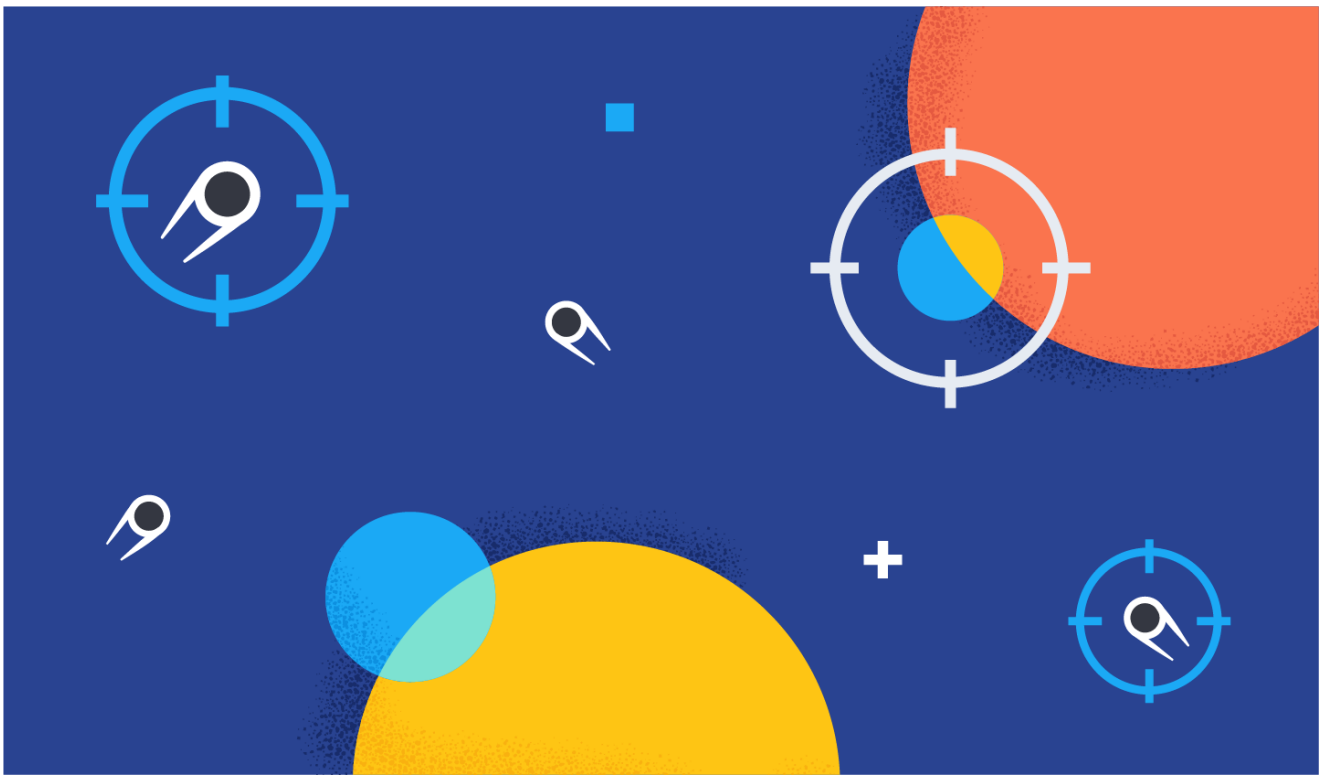
Elastic Security prevents 100% of REvil ransomware samples

elastic.co/blog/elastic-security-prevents-100-percent-of-revil-ransomware-samples

July 7, 2021



07 July 2021News

By
Jamie Butler
Share

Users of Elastic Security are protected through numerous layers of protections against the REvil ransomware that affected Kaseya VSA and its customers. Elastic Security's layered protections prevented 100% of the REvil ransomware samples tested before damage and loss could occur to the business.

We believe that detections and preventions must be layered, as no single protection works 100% of the time. There are times where detection in the SIEM/central analytics layer is the most effective, especially when you need to take signals from multiple places or correlate the activity to determine it is malicious. However, the most effective way to stop an attack is at the host.

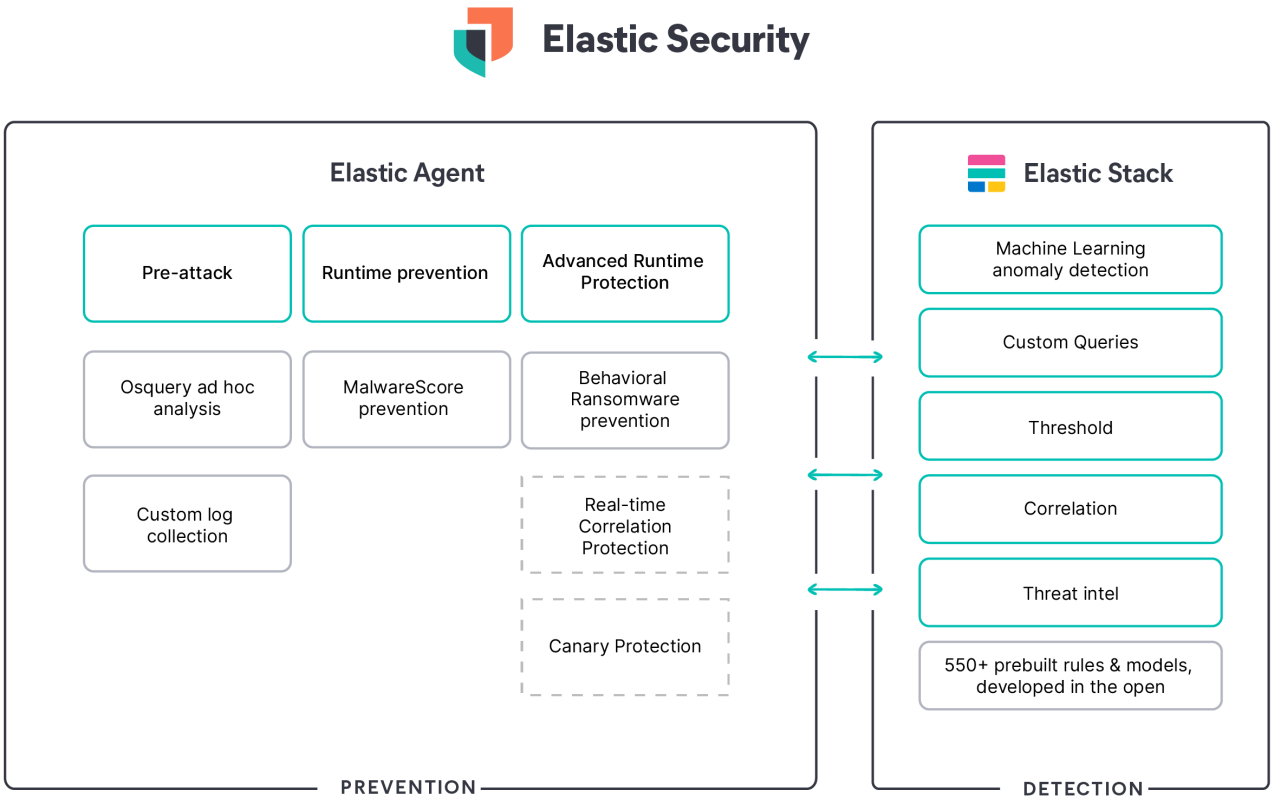
Prevention is paramount when it comes to ransomware. Teams cannot wait to be notified of an issue after their data is encrypted. Layering in the context of multiple signals from anomalous logins to unusual processes can also be telling during the early stages of a breach and help identify root cause. It is the combination of Elastic Security's SIEM, Endpoint Security, and XDR capabilities in a single solution built for limitless analysis that can protect your organization from damage and loss.

Background on Kaseya VSA supply-chain ransomware attack

On July 2, 2021, many internet sites and social media posts began warning about a ransomware attack targeting Kaseya and its customers and their customers — a supply chain attack. Kaseya bills itself as an IT management platform for IT teams and MSPs (Managed Security Providers). We have seen this type of attack in the past. The current attack compromised between 800 and 1500 victims.

Perhaps the worst part of the attack is that many of the victims are small businesses that were infected because their MSP or IT used Kaseya. The threat actors demanded $70M from Kaseya, which would be one of the largest single ransomware payouts. While this attack is alarming and perhaps unprecedented, Elastic Security has many preventions and ways to detect this attack.

Layers of defense



MalwareScore

The first layer of defense the attack hit is Elastic's signatureless malware prevention model, called MalwareScore. This extremely compact and efficient model allows Elastic Security to stop previously unknown attacks leveraging the power of machine learning using an algorithm called gradient boosted decision trees. We tested all known samples (Appendix A) and our malware prevention stopped 64.29%. It is important to note that this defense is pre-execution, stopping this attack before any attacker code can run on the system.

All Elastic Security users and Elastic Endgame users were protected by MalwareScore since model version 4.0.4000 released in March 2021.

Behavioral ransomware prevention

Elastic also constantly monitors the file system for potential signs of ransomware activity with behavioral ransomware prevention. This protection, which builds off of the lessons learned from the original Elastic Endgame implementation and has been available since the 7.12 release of Elastic Security, is an added layer of heuristic protection to stop any ransomware attack at runtime which MalwareScore may have missed. When we tested the fourteen REvil samples referenced in Appendix A, this protection had a **prevention rate of 100%**. Users of Elastic Security have been protected by behavioral ransomware prevention against these samples since the 7.12 release, while Elastic Endgame users have been protected since July 2020.

All Elastic Security users have been protected by behavioral ransomware since 7.12 released in March 2021.

All Elastic Endgame users were protected from July of last year (2020).

Security analytics

Elastic Security provides free and open threat detection capabilities as well that help address techniques used by the REvil criminal ransomware group, and which are developed in public with the community. Using information disclosed by multiple organizations as well as Elastic's own telemetry visibility, the following rules and machine-learning jobs may help those affected by this threat:

Disabling Windows Defender Security Settings via PowerShell - During initial access, REvil operators used PowerShell to disable several critical security settings in Defender and which pertain to malware detection

Enable Host Network Discovery via Netsh - REvil operators used the built-in Network Shell utility to enable local network discovery, subverting the Windows Firewall

Encoding or Decoding Files via CertUtil - REvil operators renamed the Windows CertUtil.exe application, which was then used to decode their ransomware payload

Potential DLL SideLoading via Microsoft Antimalware Service Executable - REvil operators deployed a deprecated version of Microsoft Windows Defender which was vulnerable to DLL side-loading, and which provided a mechanism to execute their decoded ransomware payload

Unusual Process for a Windows Host - REvil operators used existing utilities to disable Windows Defender, decode ransomware or enable network discovery; in environments where those utilities are rarely used, this machine learning job may generically identify these behaviors

More is on the way

Just because something is blocked today does not mean we can stop innovating on protections. Numerous soon-to-be-released protections also stopped this attack at the host. These protections, currently in diagnostic mode, were tested against the known samples.

To improve our chances of rapidly catching anomalous file modification behavior patterns typically indicative of ransomware, we have incorporated canary files into our suite of layered protections. Elastic Security is optimized to immediately detect suspicious modifications to these specially crafted files, which are placed throughout the file system in various locations which increase the odds that they are targeted at the onset of a ransomware infection.

When paired with our core behavioral ransomware prevention feature, canary files provide an effective means for reducing our mean time to detect post-execution ransomware and minimize potential adverse effects to the file system. When detonated in our testing environment, 100% of the REvil ransomware samples relating to this attack were detected by modifications to canary files.

Elastic’s commitment to your business

Our mission at Elastic Security is to protect the world’s data from attack. We are constantly innovating in the protection space to ensure our users across the world are protected from tomorrow’s attacks. The solution delivers free and open capabilities of SIEM, Endpoint Security, and XDR on a single platform built for limitless analysis, enabling organizations to prevent, detect, and respond before damage is done.

If you’re new to Elastic Security, you can experience our latest version on Elasticsearch Service on Elastic Cloud for free.

Appendix A

Below are the file hashes of the known samples of the Kaseya VSA supply-chain ransomware attack:

d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e
e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2
8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
36a71c6ac77db619e18f701be47d79306459ff1550b0c92da47b8c46e2ec0752
33bc14d231a4afaa18f06513766d5f69d8b88f1e697cd127d24fb4b72ad44c7a
df2d6ef0450660aaae62c429610b964949812df2da1c57646fc29aa51c3f031e
dc6b0e8c1e9c113f0364e1c8370060dee3fcbe25b667ddeca7623a95cd21411f
d8353cfc5e696d3ae402c7c70565c1e7f31e49bcf74a6e12e5ab044f306b4b20
d5ce6f36a06b0dc8ce8e7e2c9a53e66094c2adfc93cfac61dd09efe9ac45a75f
cc0cdc6a3d843e22c98170713abf1d6ae06e8b5e34ed06ac3159adafe85e3bd6
aae6e388e774180bc3eb96dad5d5bfefd63d0eb7124d68b6991701936801f1c7
66490c59cb9630b53fa3fa7125b5c9511afde38edab4459065938c1974229ca8
0496ca57e387b10dfdac809de8a4e039f68e8d66535d5d19ec76d39f7d0a4402
81d0c71f8b282076cd93fb6bb5bfd3932422d033109e2c92572fc49e4abc2471
8e846ed965bbc0270a6f58c5818e039ef2fb78def4d2bf82348ca786ea0cea4f
1fe9b489c25bb23b04d9996e8107671edee69bd6f6def2fe7ece38a0fb35f98e

Credit for hashes: Cado Security, Sophos, TruSec, Florian Roth, and DoublePulsar