CASE STUDY

WEBROOT
Smarter Cybersecurity

and

sinexia
Future. Today.

> Being able to automatically block malicious scripts, especially from Emotet, is a game changer for us and our client base.
>
> **Pietro Coletta, Sr. Technician**

At a Glance

Vertical
Managed Service Provider

Year Founded
2014

Title
Senior Technician:
Pietro Coletta

Endpoints Managed
1000

Website
www.sinexia.it

Key Findings

Time Savings
No longer spend 4+ hours per machine remediating due to Emotet

Efficacy
Successfully blocked numerous instances of malicious and fileless scripts, as well as Emotet

New Webroot® Evasion Shield Empowers MSP to Protect Clients from Emotet and Malicious Scripts

Background

Sinexia S.r.l. has been protecting small businesses throughout Italy from cyber threats since 2014. A mighty team of five, Sinexia has been using and managing Webroot® Business Endpoint Protection to secure every one of their clients' machines—1000 endpoints—for approximately five years. Some clients have begun using Webroot® DNS Protection as well. According to Pietro Coletta, Sr. Technician, Webroot Business Endpoint Protection is the security tool he trusts and relies on the most.

The Challenge

Although Sinexia has deployed endpoint security to every system under their management, they found some of their clients still struggled with malicious files, Trojans, and hard-to-detect script-based attacks. The unfortunate truth is that no endpoint security solution can be 100% effective, especially if end users unwittingly give attackers system access. In particular, a few of Sinexia's clients became infected with Emotet, a Trojan that typically gains access to a system first, then acts as a loader to download other kinds of malicious code, such as ransomware.

Coletta recalls that, when Emotet was present on a client's system, he noticed strange system behaviors and an uptick in scripts being installed. That's when he and his team implemented a new process to handle these cases.

"First, we would ask the client what they had been doing before the systems started acting strangely," Coletta explained. "If they told us they opened a file, especially a document containing macros, we knew it was probably Emotet or something similar. Unfortunately, that often meant we had to reimage those machines to be safe, which was time-consuming for everyone involved."

With team members spending at least four hours per machine on Emotet-related reimaging, Coletta knew something had to give. The team's productivity was starting to lag as they spent time remediating systems, instead of handling higher value work. Additionally, affected clients were getting understandably nervous, and were beginning to lose trust. But Coletta also encountered issues convincing clients that the work needed to be done, since there were no good ways to demonstrate the script-related infections to the client.

The Solution

Earlier in 2020, Webroot began beta-testing a new feature for its Endpoint Protection product, the Webroot® Evasion Shield. Designed to combat evasive script attacks, including file-based, fileless, obfuscated, and encrypted threats, the new shield also helps prevent malicious behaviors from executing in PowerShell, JavaScript, and VBScript files.

When Coletta learned about the beta test, it sounded like the very thing his customers needed. After working with Webroot to deploy the test version of the shield on his environments, he and Sinexia's clients began realizing the benefits right away.

"In just five weeks of beta-testing the Webroot® Evasion Shield, we blocked 55 malicious scripts on client machines and stopped at least three confirmed instances of Emotet, all from fileless scripts. Being able to automatically block malicious scripts, especially from Emotet, is a game changer for us and our client base."

– Pietro Coletta, Sr. Technician

In addition to the noticeable protection benefits, the new malicious script reporting capabilities available in the Webroot® management console helped Sinexia demonstrate value and improve trust with hesitant clients. "I could tell customers, 'this tool is very useful because you don't always see the effects of these attacks. You think everything is OK on the network, but it's not.' Having such improved visibility is illuminating," says Coletta.

"It's an incredible benefit to be able to call clients proactively and tell them something is wrong, even though they don't know about it yet. It's even better to be able to show them screenshots and reports so they understand that it's a real threat, and then to finish that conversation with 'and I already took care of it for you.'"

Best of all, despite still being in beta testing, the Evasion Shield didn't hinder performance. Calling the shield's operations "lightweight" and "practically undetectable", Coletta reports he experienced "no negative impact on the computers where it was running. No impact at all. Just stronger protection." Additionally, work for his teams could continue as normal during the beta, even as the COVID-19 outbreak began circulating throughout Italy.

Conclusion

Overall, Coletta would call his beta test of the Webroot Evasion Shield "a complete success." He only laments that he couldn't have started testing the feature sooner, since it would have helped other customers whose machines had to be reimaged previously, and is looking forward to receiving real-time results once the shield is released for general availability in May of 2020.

"The Webroot console is my one-stop shop, and this enhancement is exactly what we needed to keep our clients protected. That plus the level of automation will free up time for my team to focus on other business-critical tasks," Coletta says. In particular, he wants to look into partnering with an RMM provider to bring even more automation capabilities to Sinexia's operations.

"Looks like Webroot integrates with quite a few RMM providers. Good thing I now have more time to research which solution will be best for my clients."

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900