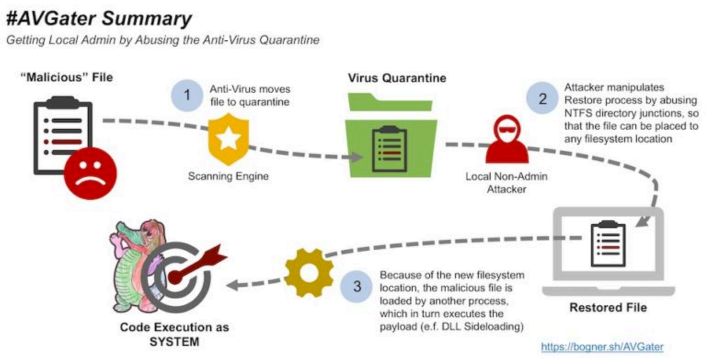
BIZ & IT —

How AV can open you to attacks that otherwise wouldn’t be possible

New AVGater flaw provided key ingredient for hacker to hijack computer.

DAN GOODIN - 11/10/2017, 1:00 AM


#AVGater Summary
Getting Local Admin by Abusing the Anti-Virus Quarantine
"Malicious" File
1
Anti-Virus moves file to quarantine
Scanning Engine
Virus Quarantine
Local Non-Admin Attacker
2
Attacker manipulates Restore process by abusing NTFS directory junctions, so that the file can be placed to any filesystem location
Restored File
3
Because of the new filesystem location, the malicious file is loaded by another process, which in turn executes the payload (e.f. DLL Sideloading)
Code Execution as SYSTEM
https://bogner.sh/AVGater

Florian Bogner

Enlarge

64

Antivirus programs, in many cases, make us safer on the Internet. Other times, they open us to attacks that otherwise wouldn't be possible. On Friday, a researcher documented an example of the latter—a vulnerability he found in about a dozen name-brand AV programs that allows attackers who already have a toehold on a targeted computer to gain complete system control.

AVGater, as the researcher is calling the vulnerability, works by relocating malware already put into an AV quarantine folder to a location of the attacker's choosing. Attackers can exploit it by first getting a vulnerable AV program to quarantine a piece of malicious code and then moving it into a sensitive directory such as C:\Windows or C:\Program Files, which normally would be off-limits to the attacker. Six of the affected AV programs have patched the vulnerability after it was privately reported. The remaining brands have yet to fix it, said Florian Bogner, a Vienna, Austria-based security researcher who gets paid to hack businesses so he can help them identify weaknesses in their networks.

Bogner said he developed a series of AVGater exploits during several assignments that called for him to penetrate deep inside customer networks. Using malicious phishing e-mails, he was able to infect employee PCs, but he still faced a significant challenge. Because company administrators set up the PCs to run with limited system privileges, Bogner's malware was unable to access the password database—known as the Security Account Manager—that stored credentials he needed to pivot onto the corporate network.

"With the help of AVGater, I gained local admin privileges," Bogner wrote in an e-mail. With full control over the employee computer his exploit provided, he had no trouble accessing the credential store, which is commonly known as a SAM database. "So AVGater was VERY useful during several of our pentests and red-teaming assignments."

Owning Antivirus

The attack worked first by getting Bogner's malicious file quarantined by the AV program running on the targeted computer. The pentester then exploited vulnerabilities in the AV programs that allowed unprivileged users to restore the quarantined files. He further abused a Windows feature known as NTFS file junction point to force the restore operation to put his malicious file into a privileged directory of Bogner's choosing. The technique took advantage of another Windows feature known as Dynamic Link Library search order. With that, Bogner's malware ran with full privileges.

Bogner initially found six AV engines that were vulnerable and privately reported the flaw to them. All of them have recently plugged the local privilege escalation hole. They are: Emisoft, Ikarus, Kaspersky, Malwarebytes, Trend Micro, and ZoneAlarm. In the past week, Bogner said he has identified seven other AV engines he believes are similarly vulnerable. He's in the process of working with the providers to understand precisely how their products are affected. To give the providers time and to prevent the vulnerabilities from being exploited maliciously in the wild, he isn't naming the AV products.

AVGater is the latest example of the way AV programs can make people susceptible to attacks that otherwise wouldn't be possible. These types of critical AV weaknesses have existed for as long as the industry has, but they didn't start to get much attention until researchers Alex Wheeler and Neel Mehta presented a talk titled 0wning Antivirus at the Blackhat security conference in 2005. They disclosed critical flaws in AV products from Symantec, McAfee, TrendMicro, and F-Secure.

Two years later, researcher Sergio Alvarez delivered a talk at the Chaos Communication Camp that disclosed flaws in products from CA eTrust, Norman, Panda, ESET, F-Secure, Avira, and Avast. In 2008, researcher Feng Xue presented two talks that aired still more vulnerabilities in an even wider list of engines.

More recently, a Google Project Zero researcher has found critical vulnerabilities in AV. In the past year, senior developers for both Chrome and Firefox have also strongly criticized AV security, with Justin Schuh, the security chief for the Google browser, calling AV "my single biggest impediment to shipping a secure browser."

FURTHER READING
This Windows Defender bug was so gaping its PoC exploit had to be encrypted

The problem with AV is that it's expected to interact with just about every kind of file, even when it's not opened. That presents a key opening for attackers, particularly when exploiting AV products that haven't been properly safeguarded with security sandboxes, software fuzzers, and similar protections. A recently fixed bug in Microsoft's Windows Defender engine, for example, allowed for code-execution attacks that could be triggered by a simple e-mail attachment, even when the recipient didn't open it.

In fairness to the AV providers, they are generally extremely quick to fix vulnerabilities once they're reported. What's more, there's little doubt that AV prevents millions of computers from being infected with ransomware, keyloggers, and other types of malware that would have had free rein over computers that didn't have the protection installed. As a general rule, people who aren't likely to be narrowly targeted in attacks are probably better off running Windows Defender or another name-brand AV engine. Journalists, lawyers, and activists, on the other hand, should weigh the benefits and risks on a case-by-case basis.

Promoted Comments

Thoughtful / Ars Praefectus / *et Subscriptor*

JUMP TO POST

> stine wrote:
>
> > **Quote:**
> > Journalists, lawyers, and activists, on the other hand, should weigh the benefits and risks on a case-by-case basis.
>
> What exactly does this mean?

I guess Dan's suggesting that if you consider yourself a target worthy of individual attention, AV might be a worse idea in some circumstances.

4793 posts | registered 12/16/2010

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 64 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS

CNMN Collection
WIRED Media Group
Use of this Site constitutes acceptance of our User Agreement (effective 1/2/14) and Privacy Policy (effective 1/2/14), and Ars Technica Addendum (effective 5/17/2012). View our Affiliate Link Policy. Your California Privacy Rights. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.