He Perfected a Password-Hacking Tool—Then the Russians Came Calling

wired.com/story/how-mimikatz-became-go-to-hacker-tool/

Andy Greenberg November 9, 2017

Five years ago, Benjamin Delpy walked into his room at the President Hotel in Moscow, and found a man dressed in a dark suit with his hands on Delpy's laptop.

Just a few minutes earlier, the then 25-year-old French programmer had made a quick trip to the front desk to complain about the room's internet connection. He had arrived two days ahead of a talk he was scheduled to give at a nearby security conference and found that there was no Wi-Fi, and the ethernet jack wasn't working. Downstairs, one of the hotel's staff insisted he wait while a technician was sent up to fix it. Delpy refused, and went back to wait in the room instead.

When he returned, as Delpy tells it, he was shocked to find the stranger standing at the room's desk, a small black rollerboard suitcase by his side, his fingers hurriedly retracting from Delpy's keyboard. The laptop still showed a locked Windows login screen.

The man mumbled an apology in English about his keycard working on the wrong room, brushed past Delpy, and was out the door before Delpy could even react. "It was all very strange for me," Delpy says today. "Like being in a spy film."

It didn't take Delpy long to guess why his laptop had been the target of a literal black bag job. It contained the subject of his presentation at the Moscow conference, an early version of a program he'd written called Mimikatz. That subtly powerful hacking tool was designed to siphon a Windows user's password out of the ephemeral murk of a computer's memory, so that it could be used to gain repeated access to that computer, or to any others that victim's account could access on the same network. The Russians, like hackers around the world, wanted Delpy's source code.

In the years since, Delpy has released that code to the public, and Mimikatz has become a ubiquitous tool in all manner of hacker penetrations, allowing intruders to quickly leapfrog from one connected machine on a network to the next as soon as they gain an initial foothold.

Benjamin Delpy

Most recently, it came into the spotlight as a component of two ransomware worms that have torn through Ukraine and spread across Europe, Russia, and the US: Both NotPetya and last month's BadRabbit ransomware strains paired Mimikatz with leaked NSA hacking tools to create automated attacks whose infections rapidly saturated networks, with disastrous results. NotPetya alone led to the paralysis of thousands of computers at companies like Maersk, Merck, and FedEx, and is believed to have caused well over a billion dollars in damages.

Those internet-shaking ripples were enabled, at least in part, by a program that Delpy coded on a lark. An IT manager for a French government institution that he declines to name, Delpy says he originally built Mimikatz as a side project, to learn more about Windows security and the C programming language—and to prove to Microsoft that Windows included a serious security flaw in its handling of passwords.

His proof-of-concept achieved its intended effect: In more recent versions of Windows, the company changed its authentication system to make Mimikatz-like attacks significantly more difficult. But not before Delpy's tool had entered the arsenal of every resourceful hacker on the planet.

"Mimikatz wasn’t at all designed for attackers. But it's helped them," Delpy says in his understated and French-tinged English. "When you create something like this for good, you know it can be used by the bad side too."

Even today, despite Microsoft's attempted fixes, Mimikatz remains an all-too-useful hacker tool, says Jake Williams, a penetration tester and founder of security firm Rendition Infosec. "When I read a threat intelligence report that says someone used Mimikatz, I say, 'tell me about one that doesn’t,'" Williams says. "Everyone uses it, because it works."

Secrets for the Taking

Mimikatz first became a key hacker asset thanks to its ability to exploit an obscure Windows function called WDigest. That feature is designed to make it more convenient for corporate and government Windows users to prove their identity to different applications on their network or on the web; it holds their authentication credentials in memory and automatically reuses them, so they only have to enter their username and password once.

While Windows keeps that copy of the user's password encrypted, it also keeps a copy of the secret key to decrypt it handy in memory, too. "It’s like storing a password-protected secret in an email with the password in the same email," Delpy says.

Delpy pointed out that potential security lapse to Microsoft in a message submitted on the company's support page in 2011. But he says the company brushed off his warning, responding that it wasn't a real flaw. After all, a hacker would already have to gain deep access to a victim's machine before he or she could reach that password in memory. Microsoft said as much in response to WIRED's questions about Mimikatz: "It’s important to note that for this tool to be deployed it requires that a system already be compromised," the company said in a statement. "To help stay protected, we recommend customers follow security best practices and apply the latest updates."

> 'When you create something like this for good, you know it can be used by the bad side, too.'

Mimkatz Creator Benjamin Delpy

But Delpy saw that in practice, the Windows authentication system would still provide a powerful stepping stone for hackers trying to expand their infection from one machine to many on a network. If a piece of malware could run with administrative privileges, it could scoop up the encrypted password from memory along with the key to decrypt it, then use them to access another computer on the network. If another user was logged into that machine, the attacker could run the same program on the second computer to steal their password—and on and on.

So Delpy coded Mimikatz—whose name uses the French slang prefix "mimi," meaning "cute," thus "cute cats"—as a way to demonstrate that problem to Microsoft. He released it publicly in May 2011, but as a closed source program. "Because you don’t want to fix it, I’ll show it to the world to make people aware of it," Delpy says of his attitude at the time. "It turns out it takes years to make changes at Microsoft. The bad guys didn’t wait."

Before long, Delpy saw Chinese users in hacker forums discussing Mimikatz, and trying to reverse-engineer it. Then in mid-2011, he learned for the first time—he declines to say from whom—that Mimikatz had been used in an intrusion of a foreign government network. "The first time I felt very, very bad about it," he remembers.

That September, Mimikatz was used in the landmark hack of DigiNotar, one of the certificate authorities that assures that websites using HTTPS are who they claim to be. That intrusion let the unidentified hackers issue fraudulent certificates, which were then used to spy on thousands of Iranians, according to security researchers at Fox-IT. DigiNotar was blacklisted by web browsers, and subsequently went bankrupt.

The Second Russian Man in a Suit

In early 2012, Delpy was invited to speak about his Windows security work at the Moscow conference Positive Hack Days. He accepted—a little naively, still thinking that Mimikatz's tricks must have already been known to most state-sponsored hackers. But even after the run-in with the man in his hotel room, the Russians weren't done. As soon as he finished giving his talk to a crowd of hackers in an old Soviet factory building, another man in a dark suit approached him and brusquely demanded he put his conference slides and a copy of Mimikatz on a USB drive.

Delpy complied. Then, before he'd even left Russia, he published the code open source on Github, both fearing for his own physical safety if he kept the tool's code secret and figuring that if hackers were going to use his tool, defenders should understand it too.

As the use of Mimikatz spread, Microsoft in 2013 finally added the ability in Windows 8.1 to disable WDigest, neutering Mimikatz's most powerful feature. By Windows 10, the company would disable the exploitable function by default.

But Rendition's Williams points out that even today, Mimikatz remains effective on almost every Windows machine he encounters, either because those machines run outdated versions of the operating system, or because he can gain enough privileges on a victim's computer to simply switch on WDigest even if it's disabled.

"My total time-on-target to evade that fix is about 30 seconds," Williams says.

In recent years, Mimikatz has been used in attacks ranging from the Russian hack of the German parliament to the Carbanak gang's multimillion dollar bank thefts. But the NotPetya and BadRabbit ransomware outbreaks used Mimikatz in a particularly devious way: They incorporated the attacks into self-propagating worms, and combined it with the EternalBlue and EternalRomance NSA hacking tools leaked by the hacker group known as Shadow Brokers earlier this year.

Those tools allow the malware to spread via Microsoft's Server Message Block protocol to any connected system that isn't patched against the attack. And along with Mimikatz, they added up to a tag-team approach that maximizes those automated infections. "When you mix these two technologies, it’s very powerful," says Delpy. "You can infect computers that aren’t patched, and then you can grab the passwords from those computers to infect other computers that *are* patched."

> 'I think we must be honest: If it wasn't Mimikatz there would be some other tool.'

Nicholas Weaver, UC Berkeley

Despite those attacks, Delpy hasn't distanced himself from Mimikatz. On the contrary, he has continued to hone his creation, speaking about it publicly and even adding more features over the years. Mimikatz today has become an entire utility belt of Windows authentication tricks, from stealing hashed passwords and passing them off as credentials, to generating fraudulent "tickets" that serve as identifying tokens in Microsoft's Kerberos authentication system, to stealing passwords from the auto-populating features in Chrome and Edge browsers. Mimikatz today even includes a feature to cheat in Windows' Minesweeper game, pulling out the location of every mine in the game from the computer's memory.

Delpy says that before adding a feature that exploits any serious new security issue in Windows, he does alert Microsoft, sometime months in advance. Still, it has grown into quite the repository.

"It's my toolbox, where I put all of my ideas," Delpy says.

A Bitter Password-Protection Pill

Each of those features—the Minesweeper hack included—is intended not to enable criminals and spies but to demonstrate Windows' security quirks and weaknesses, both in the way it's built and the way that careless corporations and governments use it. After all, Delpy says, if systems administrators limit the privileges of their users, Mimikatz can't get the administrative access it needs to start hopping to other computers and stealing more credentials. And the Shadow Brokers' leak from the NSA in fact revealed that the agency had its own Mimikatz-like program for exploiting WDigest—though it's not clear which came first.

"If Mimikatz has been used to steal your passwords, your main problem is not Mimikatz," Delpy says.

Mimikatz is nonetheless "insanely powerful," says UC Berkeley security researcher Nicholas Weaver. But he says that doesn't mean Delpy should be blamed for the attacks it's helped to enable. "I think we must be honest: If it wasn't Mimikatz there would be some other tool," says Weaver. "These are fundamental problems present in how people administer large groups of computers."

And even as thieves and spies use Mimikatz again and again, the tool has also allowed penetration testers to unambiguously show executives and bureaucrats their flawed security architectures, argues Rendition security's Williams. And it has pressured Microsoft to slowly alter the Windows authentication architecture to fix the flaws Mimikatz exploits. "Mimikatz has done more to advance security than any other tool I can think of," Williams says.

Even Microsoft seems to have learned to appreciate Delpy's work. He's spoken at two of the company's Blue Hat security conferences, and this year was invited to join one of its review boards for new research submissions. As for Delpy, he has no regrets about his work. Better to be hounded by Russian spies than to leave Microsoft's gaping vulnerability a secret for those spies alone to exploit.

"I created this to show Microsoft this isn't a theoretical problem, that it’s a real problem," he says. "Without real data, without *dangerous* data, they never would have done anything to change it."