Playing nice? FireEye CEO says U.S. malware is more restrained than adversaries'

By Zaid Shoorbajee

Published: 2018-06-01 · Archived: 2026-04-05 17:27:30 UTC

Malware used by the United States in offensive cyber-operations plays "nice" when compared to other nation-state malware, according to FireEye CEO Kevin Mandia.

Speaking at the Cyber Threat Intelligence Forum produced by Scoop News Group on Thursday, Mandia said when FireEye analyzes malware from state-backed hackers, the company usually finds elements of public policy baked into operations. Certain tells in the malware's behavior or the code itself can be indicative of which state is behind it.

"We find malware that sometimes has a time to live and then it doesn't run anymore. I wonder who would do that," Mandia said on stage. "Probably [the U.S.] because we're the nicest hackers in cyberspace, besides maybe China."

The U.S. and China are more disciplined in their operations than adversaries like North Korea and Russia, who are instead unrestrained, he said.

"We see guardrails on malware from nations like the United States, but do we see guardrails on malware from Russia? No."

Other experts, including former U.S. officials, contend that the U.S. can be similarly unrestrained and careless in cyberspace. They point to one specific case that's widely attributed to the U.S. known as "Stuxnet," which originally targeted but quickly spread beyond an Iranian nuclear enrichment facility.

Mandia went on to describe an unspecified North Korean cyber-operation that when it detected someone was investigating, the malware rewrote the victim's hard drive. Such properties are indicative of North Korea's attitude toward systems they compromise, Mandia said.

"That's annoying to deal with, but that's a policy decision. They don't care what they destroy when they compromise something," he said. "And I have a funny suspicion with our lawyers looking over their shoulders with all of our offensive capability, we absolutely do care and we're not going to have collateral damage in cyberspace."

Mandia told CyberScoop in an interview after his keynote that the U.S.'s behavior could change soon. CyberScoop recently reported that officials inside the National Security Council are pressing for more offensive measures on the heels of U.S. Cyber Command's recent elevation to a fully independent combatant command.

"My gut, just pure gut, not fact based — [U.S. Cyber Command] will probably break the niceties," Mandia told CyberScoop. "In cyberspace, everyone else is breaking [laws]. Nobody wants to over escalate, however the next

war will be fought with a cyber component. We'll have to be ready for that."

The public remarks cracked a window into how U.S. cybersecurity companies deal with malware that appears to originate from the U.S. or allied governments.

Mandia, for example, told CyberScoop that before publishing a public threat intelligence report, FireEye will typically tip off intelligence officials from the Five Eyes alliance about the release. If FireEye detects malware on a customer's system that researchers think is from the U.S. or an allied country, it will remove it. But Mandia said such malware ought to be stealthier.

"If friendlies get caught by our detection, then in my opinion is they just need to get better," Mandia said. "We're going to protect our clients first and foremost."

In March, Russian cybersecurity company Kaspersky Lab released information on a operation referred to as "Slingshot," which covered malware that was spying on victims located in the Middle East. As CyberScoop previously reported, Slingshot was a U.S. counterterrorism operation aimed at capturing terrorism targets. Kaspersky's report subsequently burned the operation.

In a press briefing, FireEye executives said that the company treats all cyberthreats the same, but uses discretion when it comes to public disclosure.

"We respond to breaches all over the world. There are certain times when we think it's potentially a friendly that was behind it," said Charles Carmakal, a vice president with Mandiant, FireEye's incident response subsidiary. "From our investigative perspective we treat it as if it was a threat actor. We help our clients eradicate the threat actor from their environment."

But even with removing a threat from a customer's system, officials said the company would stop short of going public. Ron Bushar, a vice president at FireEye, compared the action to publicly disclosing a zero-day vulnerability without giving the affected organization a chance to fix the issue.

"I think there's a difference between public disclosure and investigative support, and I think there's important standards or best practices that we tend to follow," Bushar said. "And certainly before you go public with anything … there has to be a consideration of what the impacts are both from a government perspective and what those impact could be to your client and to the organization conducting those operations."

Another FireEye executive, John Hultquist, director of threat analysis, said that publicly outing a U.S. cyber-espionage operation, especially a counterterrorism effort, would cross a line that goes beyond quietly dealing with the issue for a client.

"I see counter terrorism stuff all the time," said Hultquist. "There's a difference, you know, between stopping it and publishing it for everyone to see."

Greg Otto and Chris Bing contributed to this report.