SUBSCRIBE

SC Media > Home > Security News > Malware > NCR confirms malware in lab environment, says clients not at risk

August 27, 2020

NCR confirms malware in lab environment, says clients not at risk

Bradley Barth

Follow @bbb1216bbb

String of ATMs seen at Hartsfield-Jackson Atlanta International Airport. A trojan infected NCR Corporation, potentially posing a supply chain risk to customers of the popular point-of-sale and ATM software developer.(Photo by: Jeffrey Greenberg/Universal Images Group via Getty Images)

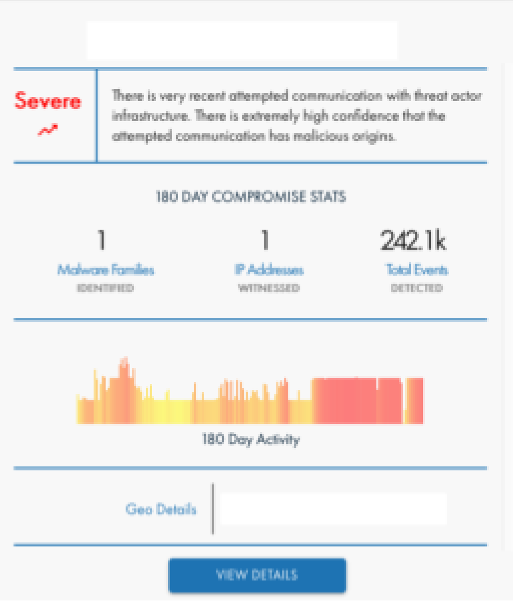
NCR Corporation has confirmed to SC Media that it found malware-infected computers in an isolated non-production lab environment outside of the U.S., but claims its clients were never at risk of a secondary infection.

The confirmation came after the CEO of cybersecurity firm Prevailion exclusively told SC Media that a trojan had infected the popular point-of-sale and ATM software developer, and expressed concern that this could potentially pose a supply-chain risk to customers.

Prevailion CEO Karim Hijazi identified the malware as Lethic, an old botnet threat that dates back to roughly 2008. While traditionally it has been used to distribute spam, it has full trojan capabilities including remote access, lateral movement, and the downloading of additional payloads. While Lethic is not new to the scene, Hijazi noted that often such malwares are repackaged so that conventional anti-virus tools won't catch them.

Hijazi said Prevailion, which monitors criminal command-and-control infrastructure for confirmed compromise activity, witnessed more than 180 days of C2 beaconing activity stemming from an IP address traced to NCR in Atlanta, home to the tech company's headquarters.

"It's been going on for an incredibly long time from our perspective… and it looks like there's been even an uptick in terms of the frequency and cadence lately," said Hijazi, noting that Prevailion has counted approximately 242,000 C2 beacons received from NCR's IP address over the course of the infection.



Severe

There is very recent attempted communication with threat actor infrastructure. There is extremely high confidence that the attempted communication has malicious origins.

180 DAY COMPROMISE STATS

1	1	242.1k
Malware Families IDENTIFIED	IP Addresses WITNESSED	Total Events DETECTED

"It has consistently moved up to a severe state, from our perspective, because… the longer something has time to persist in an environment, the more severe it actually is, because it has more time to do damage and has more doors that it can open up," Hijazi continued.

In an official statement from the company, NCR disputed aspects of Prevailion's findings, saying "We have no evidence of actual command-and-control traffic leaving our network." Prevailion has held firm on its initial assessment, however.

NCR's assertion that the infection took place outside the U.S. also runs contrary to Prevailion's statement that the malicious activity was traced to an NCR IP address in Atlanta. But NCR CISO Bob Varnadoe had an explanation for this: "I can't get into the specifics of how our internal network operate, but… all of the IP addresses assigned to the company are registered under NCR's name with our corporate headquarters address," said Varnadoe. "So what might look like – from the registration information – Atlanta, Georgia, is just because that's our headquarters address."

In its statement, NCR said that it's taking the infection seriously and "working with cyber security risk management and network experts to assess" the situation.

The statement continues: "All NCR systems and operations are functioning normally. Additionally, we have no indication that our supply chain distribution facilities or customers have been impacted. These computers are not part of our supply chain networks. Furthermore, our production and distribution facilities including but not limited to POS and ATM are on separate networks with comprehensive security controls, including malware protection."

This is significant because Hijazi had expressed concern that the trojan could have compromised NCR in such a way to spread malware to the $6.92 billion company's clients – perhaps through trojanized POS or ATM software updates.

"Any organization they may be connected to could also be impacted, so this is a contagious scenario," said Hijazi prior to NCR's statement. "That infection could island hop effectively from them to another party or vice versa – they may have contracted it from others. We don't really know. The concerning part of this is that, obviously, any organization sharing data with someone like NCR could run the risk of having that data stolen by way of these tools."

Prevailion had not alerted NCR of the infection, but SC Media reached out to the company to disclose the issue and request comment.

Varnadoe did not confirm if the affected computers were infected with Lethic, what kind of activities the malware was engaged in, and what kinds of data might have been accessible through the compromised lab environment. "We still have analysis ongoing. What we saw was DNS request traffic. At no time did we actually see command-and-control traffic," he said.

Asked by SC Media if the non-production lab is not the type of environment that would likely involve customer or client information, Varnadoe replied, "Correct." Asked if data related to internal projects, lab work or intellectual property may have been put at risk, Varnadoe said, "I probably have to get back to you on that conclusion that at this point." When further pressed, he added, "I think we need to do more analysis, before I feel comfortable commenting on that."

Prevalion followed up with SC Media on late Friday, revealing that the company has been in contact with NCR's security team and incident team. While Hijazi said the company applauds NCR "for their quick and diligent response to the compromise," he also said that "we do disagree with some of the public comments they have made about this compromise."

When NCR claims there is no evidence of C2 traffic leaving its network, "what NCR is overlooking is that these DNS requests are successfully being collected outside of their network, by us as well as the adversary," said Hijazi. "We are not the only ones seeing this call. It is likely calling to a round-robin of C2s. The reason why NCR may not see this as complete communications with the C2 is because Prevailion does not reply to the beacon requests. We simply passively collect them. Since there were no apparent resolutions to the DNS requests, there is no way NCR could determine these requests were successful."

Earlier this month, Prevailion publicly reported that it also saw evidence of a network compromise and malware infection at the cruise operator Carnival for a period spanning from Feb. 2 through June 6, 2020.

This story was edited from the original version to incorporate comments from NCR and follow-up comments from Prevailion.

TOPICS: CYBERCRIME MALWARE

Back to Top ↑

COMPANY INFO

About Us

SC Corporate News

Meet the Team

Advisory Board

Contact Us

PRODUCT REVIEW

About Product Review

Group Tests

FAQ

Licensing & Product Reviews

USER CENTER

Videos

Executive Insight Guidelines

Subscribe

Editorial Calendar

Media kit

OTHER SC SITES

RiskSec Conference

SC Resource Library

SC Online Events

SC Awards