“RobbinHood” ransomware takes down Baltimore City government networks

By Sean Gallagher

Published: 2019-05-08 · Archived: 2026-04-05 19:10:35 UTC

Systems at a number of Baltimore’s city government departments were taken offline on May 7 by a ransomware attack. As of 9:00am today, email and other services remain offline. Police, fire, and emergency response systems have not been affected by the attack, but nearly every other department of the city government has been affected in some way.

Calls to the city’s Office of Information Technology are being answered by a recording stating, “We are aware that systems are currently down. We are working to resolve the issue as quickly as possible.”

Lester Davis, a spokesperson for Baltimore’s Mayor’s office, told the Baltimore Sun’s Ian Duncan that the attack was similar to one that hit Greenville, North Carolina, in April.

Baltimore Chief Information Officer Frank Johnson confirmed in a press conference today that the malware was “the very aggressive RobbinHood ransomware” and that the FBI had identified it as a “fairly new variant” of the malware. This new variant of RobbinHood emerged over the past month.

Security researcher Vitali Kremez, who recently reverse-engineered a sample of RobbinHood, told Ars that the malware appears to target only files on a single system and does not spread through network shares. “It is believed to be spread directly to the individual machines via psexec and/or domain controller compromise,” Kremez said. “The reasoning behind it is that the ransomware itself does not have any network spreading capabilities and is meant to be deployed for each machine individually.”

That would mean that the attacker would need to already have gained administrative-level access to a system on the network “due to the way the ransomware interacts with C:\Windows\Temp directory,” Kremez explained.

In addition to requiring execution on each individually targeted machine, RobbinHood also requires that a public RSA key already be present on the targeted computer in order to begin encryption of the files. “That means that the attacker likely deploys it in multiple steps, from obtaining access to the network in question, moving laterally to obtain administrative privileges for a domain controller or via psexec, deploy and save public RSA key and ransomware on each machine and then execute it,” Kremez noted.
