“RobbinHood” ransomware takes down Baltimore City government networks

arstechnica.com/information-technology/2019/05/baltimore-city-government-hit-by-robbinhood-ransomware/

Sean Gallagher

Enlarge / Most of Baltimore City's networks were shut down as a ransomware attack took down mail servers and other systems at a number of city departments on May 7.

Alex Wroblewski / Getty images

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.”

> #BCRPALERT: BCRP is experiencing network and email outages. We apologize for the delay in all communications and are working to solve the problem. Please know our online payment, permit, program registration and service requests are currently effected. pic.twitter.com/vzXYnEqi7M
>
> — Baltimore Rec & Parks (@RecNParks) May 7, 2019

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.

Before it begins encryption, RobbinHood malware shuts down all connections to shared network directories with a `net use * /DELETE /Y` command and then runs through 181 Windows service shutdown commands—including the disabling of multiple malware-protection tools, backup agents, and email, database, and Internet Information Server (IIS) administrative services. That string of commands—which starts with an attempt to shut down Kaspersky's AVP agent—would create a lot of noise on any management system monitoring Windows systems' event logs.

Just over a year ago, Baltimore's 911 system was attacked by ransomware when maintenance on the city's networks briefly left gaps in a firewall. The firewall change was apparently only four hours old before the attackers exploited it—likely through an automated scan.

Johnson insisted that the city's information security provisions had been audited and were up to date. "We've been assessed several times since I've been here, and we've gotten multiple clean bills of health," he said. "We have a very good capability. Unfortunately, it's a race between bad actors and the cyber security industry."

In his press conference, Baltimore’s new mayor, Bernard “Jack” Young, said it was uncertain how long the city's systems would be offline. "There is a backup system with the IT department," he said, "but we can't just go and restore because we don’t know how far back the virus goes. So I don’t want people to think that Baltimore doesn’t have a backup."

In the meantime, Young said, city employees would have to switch to doing things manually. If city workers are idle for a substantial amount of time, Young said that he might ask them to "help clean up the city."