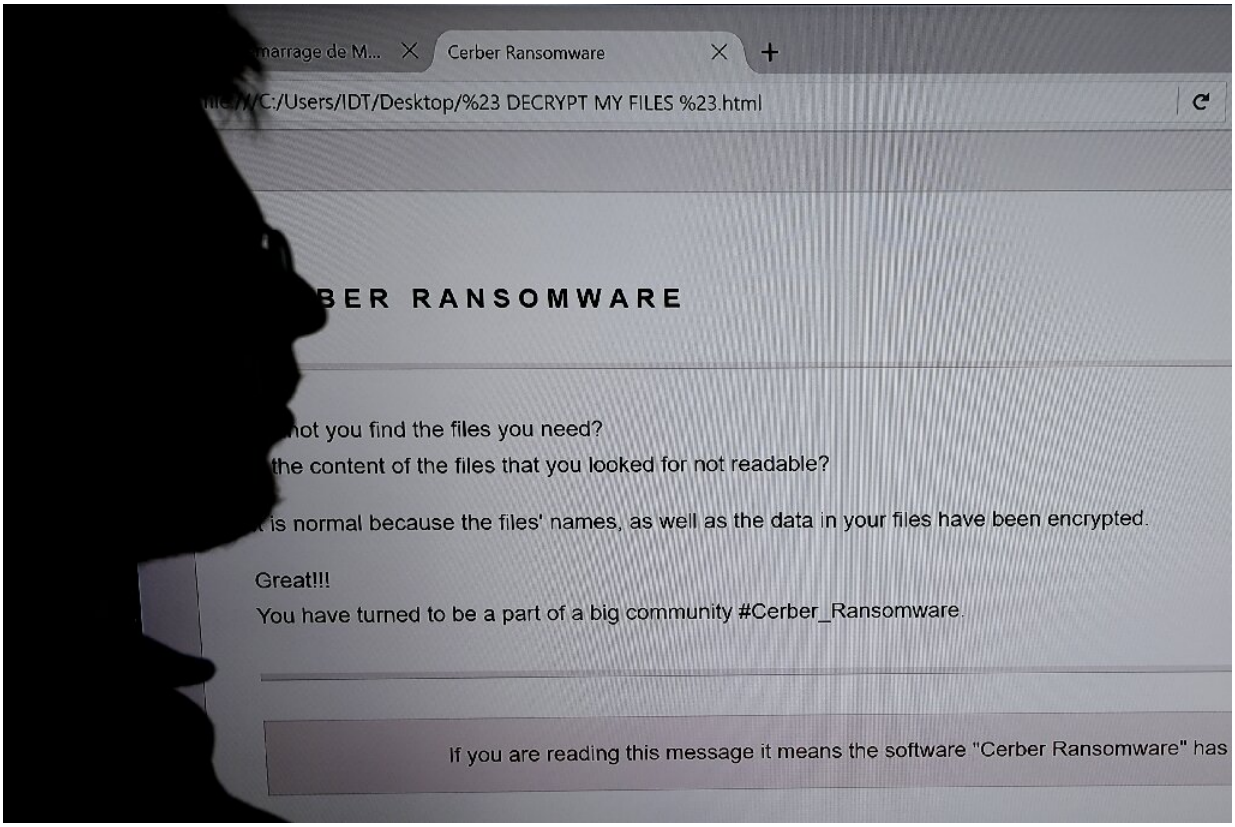
As ransomware rages, debate heats up on response

July 14 2019, by Rob Lever



Ransomware attacks have crippled many municipal and corporate networks and created difficult choices on whether to pay the hackers to unlock data

City services in Baltimore, Maryland, were paralyzed earlier this year when a ransomware attack locked up computer networks and made it

impossible for residents to make property transactions or pay their municipal bills.

Officials refused to meet hacker demands for a ransom of $76,000 to unlock the systems, but have been saddled with an estimated $18 million in costs of restoring and rebuilding the city's computer networks.

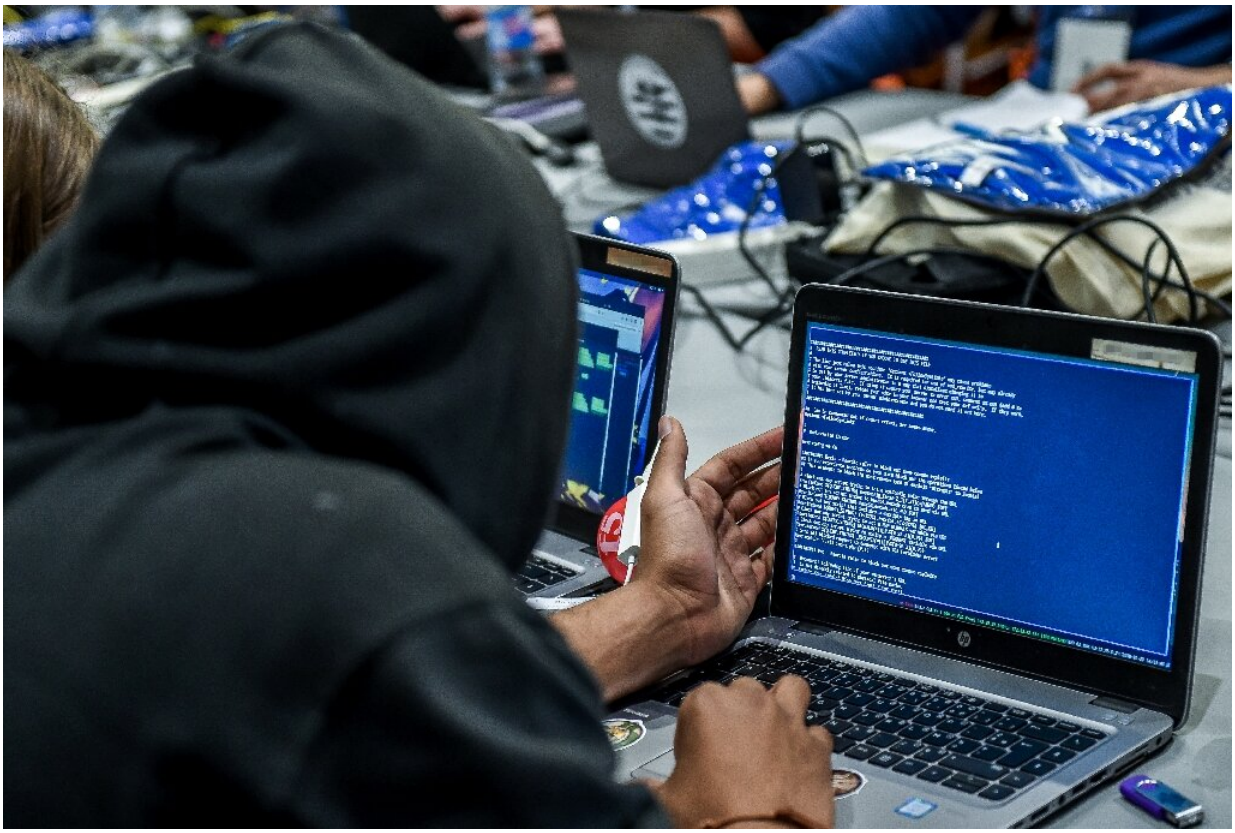
The dilemma in Baltimore and in a similar case in Atlanta a year earlier highlight tough choices faced by cities, hospitals and corporations hit by ransomware, which can shut down critical services for organizations with dated or vulnerable computer networks.

Two Florida cities reportedly paid a total of $1 million in ransom this year, after which a new attack by the same group hit the state court system in Georgia.

Globally, losses from ransomware rose by 60 percent last year to $8 billion, according to data compiled by the Internet Society's Online Trust Alliance.

At least 170 county, city or state government systems have been hit since 2013, with 22 incidents this year, according to the US Conference of Mayors, which adopted a resolution opposing ransomware payments.

"We're seeing more attacks against cities because it's clear cities are ill-prepared, and even if they know what's going on they don't have the funds to fix it," said Gregory Falco, a researcher at Stanford University specializing in municipal network security.



Some analysts say ransomware attacks may have political motivations as well as financial ones

Epidemic proportions

Frank Cilluffo, head of Auburn University's Center for Cyber and Homeland Security, said the attacks have reached epidemic levels.

"The scale and scope of the problem is striking, affecting everywhere from relatively robust states to major metropolitan areas to smaller cities and counties," Cilluffo told a congressional hearing last month.

"Targets include police and sheriff departments, schools and libraries,

health agencies, transit systems, and courts... no jurisdiction is too small or too large to go unaffected."

Ransomware has been a thorny cybersecurity issue for several years in the US and globally, marked by global ransomware attacks known as "WannaCry" and "NotPetya."

Health care institutions have been frequent victims, and Hollywood Presbyterian Medical Center revealed in 2016 it paid $17,000 to hackers to decrypt important data.

The French Interior Ministry said in a recent report authorities responded to some 560 ransomware incidents in 2018 but also noted that most incidents are unreported.

The same ministry report said hackers have shifted their strategy from attacking many systems with demands for small ransoms to more targeted attacks with higher potential payout.

Global losses from ransomware amounted to some $8 billion in 2018, according to a recent study

Pay or resist?

While the FBI and others warn against paying ransoms, some analysts say there is no clear answer for victims when critical data is locked.

"You have to do what's right for your organization," Falco said. "It's not the FBI's call. You might have criminal justice information, you could have decades of evidence. You have to weigh this for yourself."

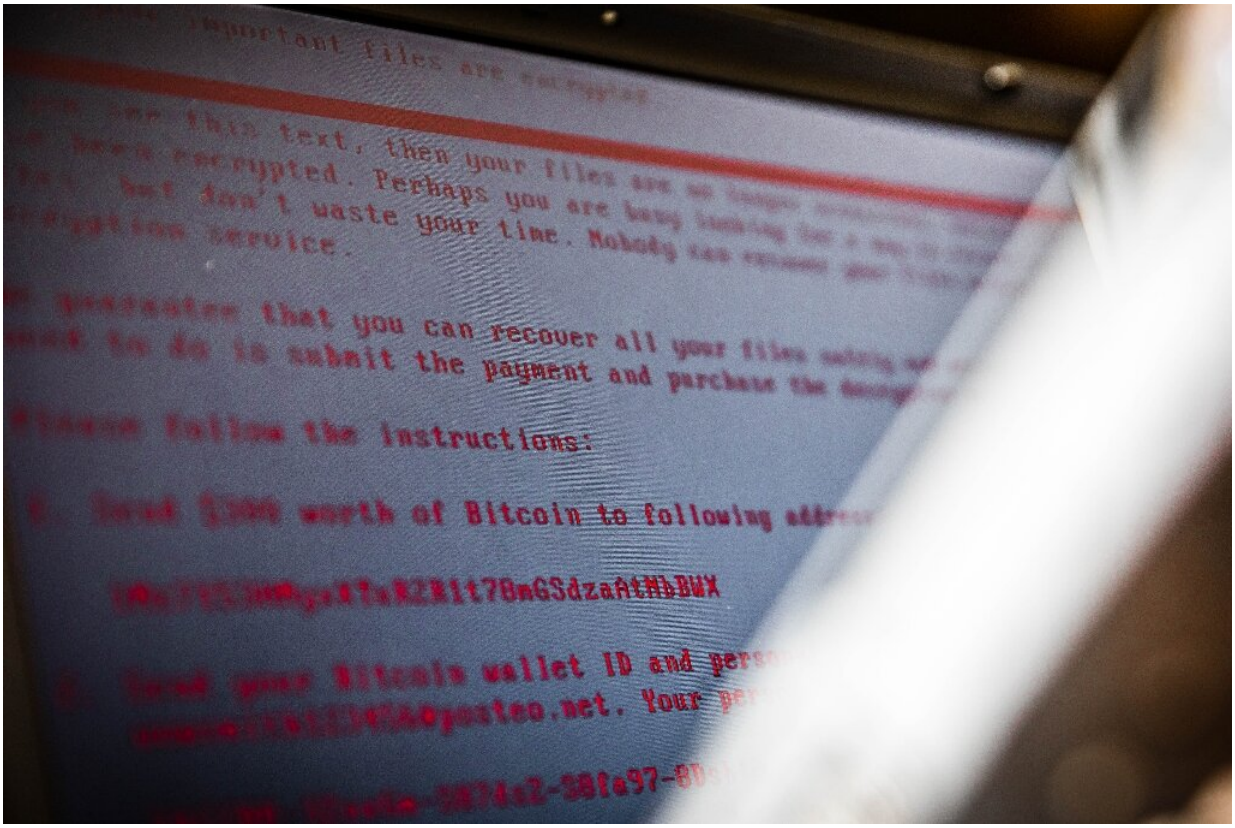
Josh Zelonis at Forrester Research offered a similar view, saying in a blog post that victims need to consider paying the ransom as a valid

option, alongside other recovery efforts.

But Randy Marchany, chief information security officer for Virginia Tech University, said the best answer is to take a hardline "don't pay" attitude.

"I don't agree with any organization or city paying the ransom," Marchany said.

"The victims will have to rebuild their infrastructure from scratch anyway. If you pay the ransom, the hackers give you the decryption key but you have no assurance the ransomware has been removed from all of your systems. So, you have to rebuild them anyway."



A global cyberattack in 2017 infected more than 200,000 victims in more than 150 countries with ransomware, including Britain's state-run National Health Service

Prevention is best

Victims often fail to take preventive measures such as software updates and data backups that would limit the impact of ransomware.

But victims may not always be aware of potential remedies that don't involve paying up, said Brett Callow of Emsisoft, one of several security firms that offer free decryption tools.

"If the encryption in ransomware is implemented properly, there is a zero chance of recovery unless you pay the ransom," Callow said.

"Often it isn't implemented properly, and we find weaknesses in the encryption and undo it."

Callow also points to coordinated efforts of security firms including the No More Ransom Project, which partners with Europol, and ID Ransomware, which can identify some malware and sometimes unlock data.

Analysts point out that ransomware attacks may be motivated by more than just money. Two Iranians were charged last year in the attack on Atlanta that prosecutors said was an attempt to disrupt US institutions.

"Attackers which aren't such big fans of the US might want to cause economic disruption," Falco said.

"Instead of trying to take down the whole electric grid, they may try to create chaos in a number of cities."