

WATCH LIVE: TRUMP DELIVERS FOREIGN POLICY SPEECH GET ALERTS 



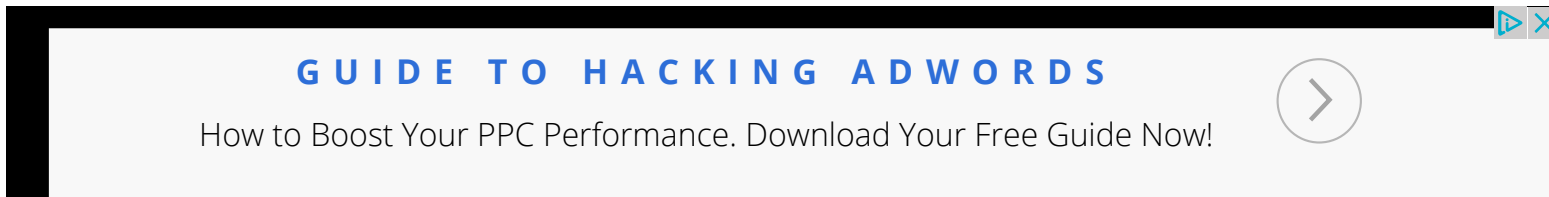
HOME TOP VIDEOS DECISION 2016 MORE 



advertisement

GUIDE TO HACKING ADWORDS

How to Boost Your PPC Performance. Download Your Free Guide Now!



NEWS > U.S. NEWS

WORLD INVESTIGATIONS CRIME & COURTS ASIAN AMERICA LATINO NBCBLK

NEWS APR 26 2016, 6:53 AM ET

Ransomware Hackers Blackmail U.S. Police Departments

by CHRIS FRANCESCANI

SHARE    

Cyber criminals who have forced U.S. hospitals, schools and cities to pay hundreds of millions in blackmail or see their computer files destroyed are now targeting the unlikeliest group of victims — local police departments.

Eastern European hackers are hitting law enforcement agencies nationwide with so-called "ransomware" viruses that seize control of a computer system's files and encrypt them. The hackers then hold the files hostage if the victims

don't pay a ransom online with untraceable digital currency known as Bitcoins. They try to maximize panic with the elements of a real-life hostage crisis, including ransom notes and countdown clocks.

If a ransom is paid, the victim gets an emailed "decryption key" that unlocks the system. If the victim won't pay, the hackers threaten to delete the files, which they did last year to departments in Alabama and New Hampshire. That means evidence from open cases could be lost or altered, and violent criminals could go free.

Since 2013, hackers have hit departments in at least seven states. Last year, five police and sheriff's departments in Maine were locked out of their records management systems by hackers demanding ransoms.


Ransomware crimes on all U.S. targets are soaring. In just the first three months of 2016, attacks increased tenfold over the total entire previous year, costing victims more than \$200 million. Authorities stress that this number only represents known attacks. One federal law enforcement official told NBC News that the "large majority" of attacks go unreported.

The viruses - most of which come from Russia and Eastern Europe — are typically so impenetrable that even FBI agents have at times advised victims to just pay up and get their data back.

Police computers, however, are especially vulnerable to ransomware, because many small departments have ancient systems.

One chief acknowledged to NBC News that when his department's computers were attacked last year, they were running on DOS, an outdated disc-operating system that dates back to the early 1980s.



A ransom note sent by hackers to a ransomware victim.  Cisco Talos

"Think about it," said Robert Siciliano, an online safety expert for Intel Security. "You have local law enforcement [which is] provided grants for all kinds of advanced technologies that often revolve around weaponry, but then when it comes to upgrading their desktops laptops — they may not be up to speed."

Said Siciliano, "It's not unheard of to see a Windows XP or Vista still in action in a law enforcement environment."

'We Are Cops. We Generally Don't Pay Ransoms'

An attack commonly begins when a person opens a piece of malware disguised as a recognizable, sometime personalized e-mail attachment. Once opened, it freezes data block by block until everything is locked.

Then, a ticking countdown clock will often appear on a victim's screen, experts said, with a ransom demand and deadline. Hackers nearly always demand Bitcoins.

Some digital ransom notes include user-friendly instructions on how to buy Bitcoins online, and direct targets to websites that broker anonymous, peer-to-peer financial exchanges.

The attacks are increasingly forcing police chiefs into frustrated deliberations over whether or not — against all their training and instincts — to reward extortionists whose identity they may never know.

"My initial reaction was 'No way!'" said Sheriff Todd Brackett of Lincoln County, Maine, whose system was frozen last spring. After "48 long hours," Brackett reluctantly paid.

"We are cops," he said with a sigh. "We generally don't pay ransoms."

Last year, the police chief in Durham, New Hampshire, refused to pay, and his files were deleted. He was able to recover most of them from a backup system.

When the Collinsville, Alabama, police department was hit in 2014, the chief refused to pay. He never saw the files again.

What makes the ransoms so maddeningly tempting for cops to pay is that most attacks that have disabled police department computers have sought just a few hundred dollars.

"It's much easier to ask for smaller amounts that you are actually going to get," said Alabama criminal justice professor Diana Dolliver.

Related: Big Paydays Force Hospitals to Prepare for Ransomware Attacks

Local law enforcement agencies' computer systems can contain plenty of vital — sometimes even deeply personal — information, ranging from rape and other violent crime reports to 911 call records, case files of ongoing investigations, personnel records and access to law enforcement databases like the National Crime Information Center (NCIC), which contains criminal case information on federal, state and local investigations.

While authorities say they are not aware of attacks on local law enforcement networks that have resulted in compromised evidence, they believe it is only a matter of time.

Business Is Booming

The attacks on U.S. police are an improbable part of what experts describe as a ransomware epidemic. One new study warns that 2016 "is the year ransomware will wreak havoc on America's critical infrastructure community ...'To Pay or Not to Pay,' will be the question fueling heated debate in boardrooms across the nation."

The business of high-tech extortion is growing exponentially. Last year, the FBI received nearly 2,500 ransomware attack complaints that cost victims \$24 million. In the first three months of 2016, ransomware attacks cost Americans another \$209 million.

Yet security experts and law enforcement officials agree that the actual figures are likely much, much higher.

"There are a lot of other law enforcement agencies out there that have been affected by this...that don't want their names out there," said Jeff McCliss, a Dickson County, Tennessee--based detective whose department paid a \$622 ransom in Bitcoins.

Many known intrusions have focused on health care facilities, school systems and even small cities — targets with critical infrastructure, limited security and a constant need for access to their records.

In February, California's Hollywood Presbyterian Medical Center paid a ransom of about \$17,000 in Bitcoins, one of at least six major health care systems victimized so far this year. Last month, the city of Plainfield, New Jersey, faced a demand for about \$700 in Bitcoins to unfreeze their municipal servers.

Federal investigators say that a majority of the attacks are launched by Eastern European cyber gangs, but there have been few high-profile arrests to date because it's so hard to identify and locate the culprits.

And while early versions of ransomware had to be executed individually, by a human, experts said that today's viruses are fully automated. They are commonly disbursed like spam by the thousands, allowing hackers to execute hundreds of shakedowns simultaneously.

Vulnerabilities 'So Easy to Mitigate'

Ransomware viruses have put federal law enforcement officials in a nearly impossible position. In most cases they can't thwart the attack, apprehend the culprit or retrieve the locked data — and they know from experience that most victims who pay get their files back.

Yet they're all-too-aware that each payout encourages more extortion.

For several years, multiple federal agencies have issued warning after warning to the public and private sectors urging proper "cyber-hygiene" and stressing the simplicity of the fix — keep your software up to date and your system regularly backed up.

"This is so easy to mitigate," the federal official said.

While the FBI now explicitly advises against paying ransoms, individual agents have been known to nudge victims in that direction.

"To be honest, we often advise people to just pay the ransom," Joseph Bonavolonta, a Boston FBI cyber and counterintelligence specialist, told a security conference last fall. "The ransomware is that good."

Those comments drew headlines in the tech industry press, and prompted a clarifying statement from the FBI.

"The FBI doesn't make recommendations to companies," the agency told Naked Security last October. "[I]nstead the Bureau explains what the options are ... and how it's up to individual companies to decide for themselves the best way to proceed ... either revert to back up systems, contact a security professional, or pay."

Earlier this month, an FBI spokeswoman issued a statement to NBC News which said, in part, that "The FBI does not condone payment of ransom, as payment of extortion monies may encourage continued criminal activity, lead to other victimizations, or be used to facilitate serious crimes."

Bonavolonta could not immediately be reached for comment.

The Department of Homeland Security offers cyber-safety training to state and local governments and conducts "red team" tests on municipal systems to determine how secure they are. The FBI offers similar training in the private sector.

"It's really important for people to know [that] we can help," said Dr. Andy Ozmant, DHS assistant secretary for cybersecurity and communications. "We have a lot of resources available."

Compromised Evidence?

Experts said that ransomware attacks can have a potentially devastating impact on a municipality's criminal justice system.

"A good defense attorney is going to raise a question about whether or not evidence had been tampered with," said Dolliver. "That's the part I've actually been really watching for, but have not seen it come up in court cases."

Lincoln County law enforcement officials brought the same concerns to their local prosecutors, who concluded that none of the recovered data was ever actually breached.

So far at least, legal experts said, most ransomware cases have not necessarily tainted evidence.

"If the computer is simply held hostage but there is no evidence that any files have been altered, there will be no problem," said Steven Saltzburg, a George Washington University law professor who co-authored the 2013 Federal Criminal Procedures Litigation Manual. "If there is evidence that files have been altered, that is a problem."

'Last Laugh'

The ransomware attacks on U.S. police have left more than a few chiefs privately fuming, including Sheriff Brackett.

In a last-ditch bid to strike at least a tiny blow on behalf of U.S. law enforcement against ransomware extortionists, Brackett and his IT team paid the Bitcoin ransom, received the decryption key, cancelled the payment, and unlocked their system.

"We got the last laugh," Brackett thought to himself at the time.

Two days after his bait-and-switch scheme, hackers struck again.

This time the ransom was about \$500.

This time Brackett paid and walked away. 📺

CHRIS FRANCESCANI 

TOPICS U.S. NEWS, CRIME & COURTS, INVESTIGATIONS, SECURITY, TECH NEWS

FIRST PUBLISHED APR 26 2016, 5:35 AM ET

↓ **NEXT STORY** Abortion in Europe: How One American Exports 'War' Strategy
