http://homenewshere.com/tewksbury_town_crier/news/article_8f8ce2ba-da0d-11e4-a127-578b97102bf0.html

Police pay ransom after cyberterror attack on network

By Jayne W. Miller News Editor Jayne@YourTownCrier.com Apr 4, 2015

Tewksbury firefighters Thomas Murphy, Daniel Sawicki and Lt. Scott Keddie approach the scene of a house fire at 24 Sullivan Parkway early Saturday evening. The two-alarm blaze brought mutual aid to cover stations from Billerica and Wilmington. Photo by Rich MacDonald

Chief: “Paying ransom was the last resort”

TEWKSBURY – Last December Tewksbury Police confronted a new, and growing, frontier in cyberterrorism when the CryptoLocker ransomware virus infected the department’s network, encrypting essential department files until the town paid a $500 bitcoin ransom. In total, police systems were down between four and five days as the department worked with the FBI, Homeland Security, Massachusetts State Police, as well as private firms in an effort to restore their data without paying the ransom.

According to the U.S. Department of Homeland Security’s Computer Emergency Readiness Team (US-CERT), CryptoLocker is a malware campaign that initially surfaced in 2013. CryptoLocker is a new variant of ransomware that restricts access to infected computers and demands the victim provide a payment to the attackers in order to decrypt and recover their files. As of this time, the primary means of infection appears to be through phishing emails containing malicious attachments, phony FedEx and UPS tracking notices, and even through pop-up ads.

Police Chief Timothy Sheehan told the Town Crier that Tewksbury was hit with a newer form of CryptoLocker, for which authorities did not have the key. Though initially infected sometime on December 7, the department became aware of the malware on December 8, 2014.

This kind of malware has the ability to find and encrypt files located within shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives. If one computer on a network becomes infected, mapped network drives could also become infected, which is what happened in Tewksbury. CryptoLocker then connects to the attackers’ command and control (C2) server to deposit the asymmetric private encryption key out of the victim’s reach.

Sheehan said that they believe the virus entered the system through the Officer –In-Charge’s (OIC) computer and began looking for a large store of data. Since all the computers have mapped drives and are networked, the virus went to the largest server – in this case that housed the Computer Aided Dispatch, records management, arrest logs, calls for service, motor vehicle matters, and so on – and encrypts everything, making it impossible to access.

“It basically rendered us in-operational, with respect to the software we use to run the Police Department,” said Sheehan.

Once officers tried to access the data following the malware infection, they received a demand for a $500 bitcoin ransom sent to a web address and account that cannot be traced by the FBI, State Police, or National Security. Bitcoin is a digital, peer-to-peer, currency with military-grade cryptography. While bitcoin promises security for online transactions, it has also become the preferred currency for ransomware, because it is untraceable.

Importantly, Sheehan points out, the data stayed within department networks. This incident was not a data breach, where credit card payment information was stolen, such as those affecting Home Depot and Target.

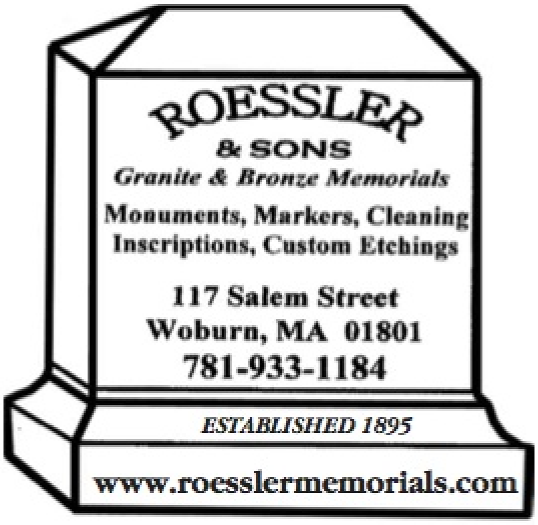
“This isn’t a breach. [The data] stays interior, but this virus encrypts it and prevents it from being readable,” said Sheehan.

Sheehan reached out to police chiefs across the state to see if anyone else had experience with this virus. A number of communities responded with similar stories. Most notably Swansea Police Department, which paid a $750 ransom in November 2013. Once alerted by Sheehan, other departments took immediate action to protect their systems, especially those with mapped drives.

Tewksbury Police sent their infected server to the Commonwealth Fusion Center in Maynard, a facility that brings federal and state services, as well as the public and private sector together, acting as the state repository for homeland security information and incident reporting.

In the meantime, the department isolated the files that were encrypted, ran virus protection on all remaining machines in the network, and were able to use their systems, but could not access saved records.

"Once hit with this kind of ransomware, only two alternatives are available,” said Sheehan. If the files cannot be decrypted, then you must go to the most recent back-up. If a recent back-up isn’t available, the ransom must be paid.



In Tewksbury's case, the back-up on an external hard drive was also corrupted. The most recent non-corrupted tape back-up was 18 months old, and simply not enough to rebuild missing information from paper reports.

Tewksbury Police teamed up with two private entities as well – Delphi Technology Solutions of Woburn and Stroz Friedberg, a digital forensics and security firm, with an office in Boston.

Delphi began working on town networks to diminish future threats and the town has contracted with the firm for 6.5 hours per week through the end of this fiscal year, dropping down to 4 hours per week proposed in the FY16 budget. In January, the Finance Committee approved transfers from the Reserve Fund to cover some of the costs of the virus, including $6,878 for a new domain server and firewall and $19,604 for professional services from Delphi.

Stroz Friedberg expressed interest in aiding the bitcoin transaction for Tewksbury, in part because this version of the CryptoLocker virus is second generation and the firm would likely encounter it in the private market. Sheehan said that while Tewksbury paid the ransom, the digital security firm handled the transaction. The firm did not accept a fee for doing the service.

Ultimately, says Sheehan, "nothing was lost."

"Nobody wants to negotiate with terrorists. Nobody wants to pay terrorists," said Sheehan. "We did everything we possibly could," including moving town departments away from mapped drives.

"It was an eye opening experience, I can tell you right now. It made you feel that you lost control of everything," said Sheehan. "Paying the bitcoin ransom was the last resort."