WBM Technology Services Community Briefing

MAY 13, 2016 Threat Alert

RANSOMWARE ATTACKS

Threat Alert

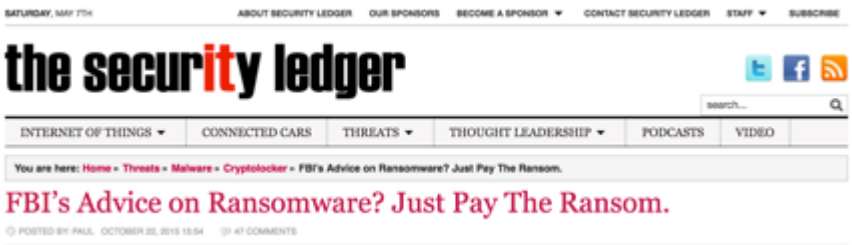
WBM has seen an extreme rise in ransomware attacks across western Canada, and this is consistent with the explosive growth in attacks throughout North America as ransomware is now clearly the single largest and fastest growing security threat of any kind to business.

Attacks in recent days have forced high profile state of emergency at Hollywood Presbyterian Hospital, downed a Michigan Electricity provider, and the new forms of the virus are so sophisticated that some FBI officials are advising infected businesses to **"just pay the ransom,"** despite there being no guarantee that the data will be decrypted, and the incentive for growth in this criminal activity.

Michigan electricity utility downed by ransomware attack
The Register - May 4, 2016
A water and electricity authority in the US State of Michigan has needed a week to recover from a **ransomware attack** that fortunately only hit its ...

Electric company hit by ransomware
Komando - May 3, 2016

Explore in depth (7 more articles)



WBM is now seeing multiple attacks per week across our customer community as of May, 2016. These attacks are detected at the firewall, prevented from spreading at the device, and the business risk is eliminated through daily backup.

In recent days we have added multiple new customers who did not have these measures in place, had been infected, and required assistance immediately, and are now protected moving forward.

It is of critical business importance that protection measures are in place.

Our commitment is to ensure the WBM client community is protected by the most sensible and comprehensive security program available in the market.

what is ransomware

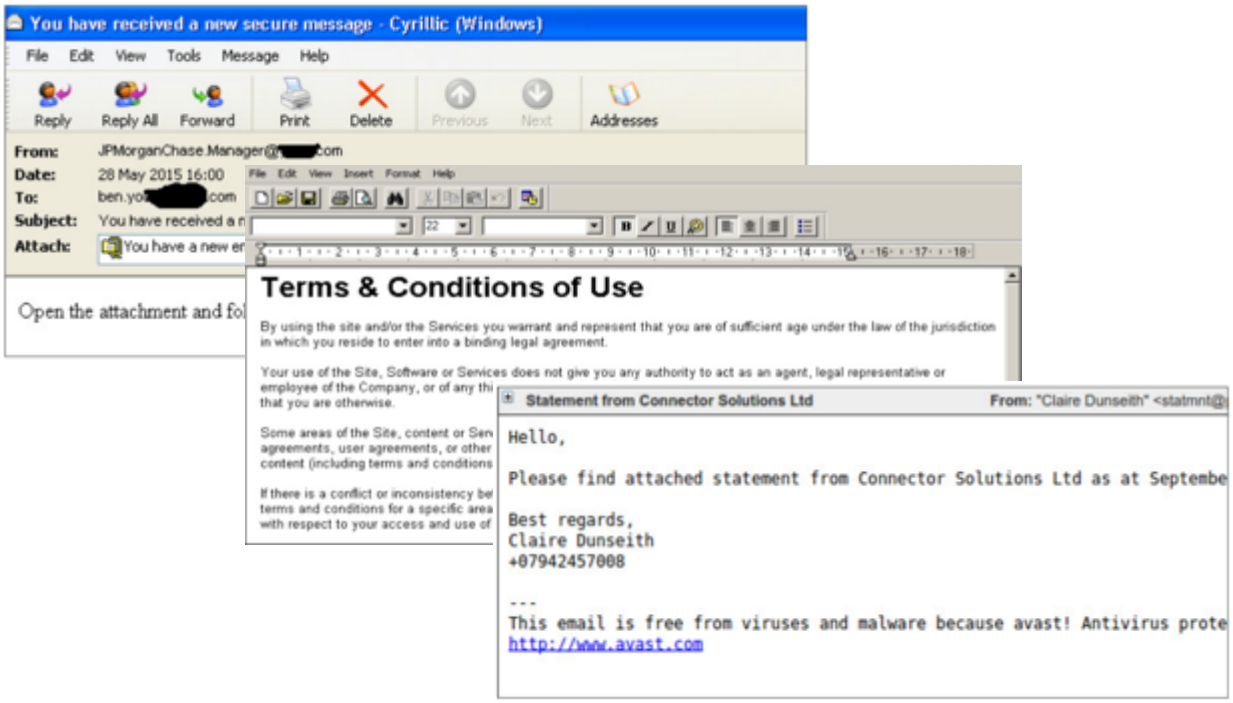
Ransomware locks down files and freezes your ability to operate by planting infection, usually in the form of emailed word, pdf, or zip attachments, but more and more often taking on much more difficult to detect exploit kits.

Once infected, your files will be locked, and screens will direct you to pay a ransom, usually in Bitcoin. The ransom will often increase as more time passes.

Ransomware first appeared in 2013 as the infamous Crypto-locker. The ransomware infections we are now seeing are much more sophisticated and must be protected against, not fixed after the fact.

Additionally, new programs and websites allow users to criminally direct the attacks to businesses they choose. These new iterations are driving the massive spike in infections, primarily in the form of CryptoWall, TorrentLocker, CTB-Locker and TeslaCrypt.

RECENT SCREEN SHOTS OF INFECTED FILES (CRYPTOWALL, TESLACRYPT, CTB LOCKER)



who is targeted

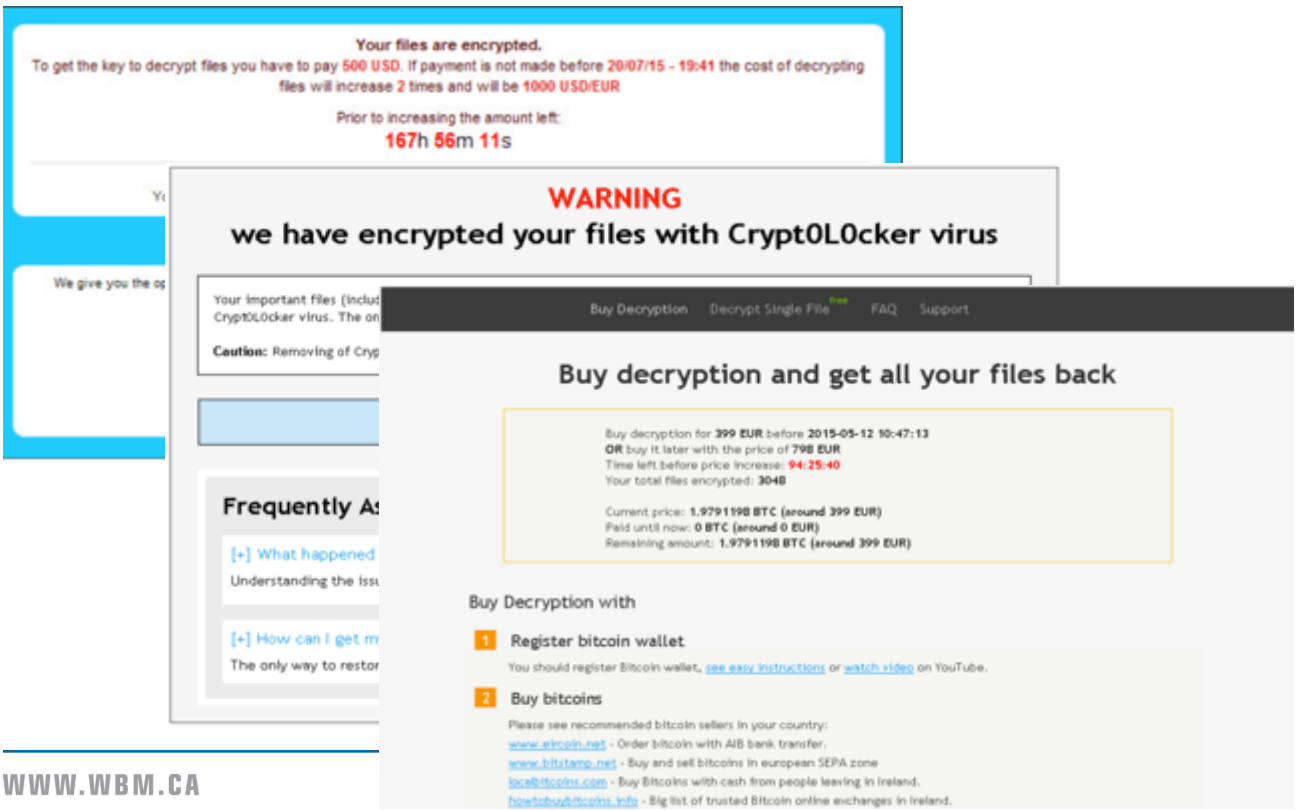
Unfortunately, North American business have become the primary target worldwide, and WBM specifically has prevented or worked to resolve infections on an alarming basis, now multiple organizations per week, which has led us to release this technical briefing.

When large organizations are hit we read about in the news, but ransomware is most effective when it can generate smaller sums of quick payments from small and medium business. When CryptoLocker first appeared in 2013, WBM met a new customer when we read about their lock down in the local news.

In recent days we have seen attacks from within our community that have required a restore to a healthy status. We have also met several new customers who were locked down, had only onsite backups on external drives, and were forced to pay a ransom before working with us to move to a protected state.

We believe that it is no longer a risk of IF your business is hit, there is now a clear reality of what is going to happen WHEN you are hit by a virus or attack.

RECENT SCREENSHOTS LOCKED SYSTEMS (CRYPTOWALL, TESLACRYPT, CTB LOCKER)



3 stage protection requirement

To protect your organization against the risk of ransomware infections, it is critical to have in place, at minimum, a three-stage security program. When all three components are in place, you are in position to stop the virus from entering your organization at the firewall, immediately act to shut down an infected computer at the device level, and restore you to a healthy state through daily monitored backup.

Next Generation Firewall: A current Next Generation Firewall (i.e. NGFW) is required to best secure you at the perimeter, working to prevent infected code from ever entering the environment. A next generation firewall provides encryption, Gateway-Antivirus, Gateway-Malware and Intrusion Protection, and is a critical and low cost security provision. WBM's NGFW service utilizes the worlds most powerful devices with ongoing monitoring and reporting, and these devices are provided as a component of your NGFW service program with no upfront purchase cost required.

Device Antivirus: Antivirus is required on your end user devices, protecting you from viruses that may have gone undetected or entered the environment in forms such as third party devices, cameras, mobile devices, or USB drives. WBM Device Antivirus involves both the software to detect and eliminates file infections at the device, and a pre approved service allowing our technical teams to receive an alert and immediately shut down the infected device to halt spread into the network.

Monitored Backup & Recovery: A fully monitored, daily backup and recovery process is required to maximize protection against this threat. Ultimately, in the event of infection, backup & recovery is the primary measure to revert back to a healthy previous state, and eliminate the need to pay a ransom. The WBM technology standard for backup & recovery process is monitored, to ensure successful backup, and provided as a service including the ability to immediately revert back to a healthy state and avoid loss of business that would otherwise occur in an infection.

key messages

- WBM is now seeing multiple attacks per week across our customer community as of May, 2016. These attacks are detected at the firewall, prevented from spreading at the device, and the business risk is eliminated through daily backup.

- We believe that it is no longer a risk of IF your business is hit, it is now clearly the reality of what is going to happen WHEN you are hit.

- In recent weeks WBM has added multiple new customers who did not have these measures in place, had been infected, and required assistance immediately, and are now protected moving forward.

- It is now of critical business importance that protection measures are in place.

- **Business intent on protecting themselves require a 3-Stage security program:**

    - **Managed Next Generation Firewall to stop intrusions and infections at the perimeter.**
    - **Managed Anti Virus to detect infections that have entered the environment and immediately stop spread into the network.**
    - **Managed backup to ensure the ability to revert back to a healthy state in the event of a lockdown.**

- The WBM business client community must be protected from this risk by the most sensible and comprehensive security program available.

whitepaper

Brett Bailey
Vice President & Partner
WBM

Ilija Stankovski
Manager of Security & Network
WBM

Jules Ouellette
Manager of Cloud Solutions
WBM