RANSOMWARE
On the Rise

Combatting the Latest Criminal Business Model Requires Multi-layered Security Approach

Ransomware at-a-Glance

- Form of malware that blocks access to files, documents, photos, etc. by encrypting them
- Attacker extorts payment from user/organization for the encryption key to decrypt and access files
- Fees are often demanded in Bitcoin, so tracing the attacker isn't feasible
- Attacks have the ability to immediately impact business productivity

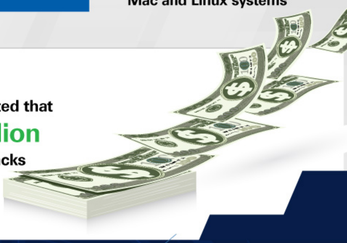
Ransomware by the Numbers
In 2015…

More than **4 million** samples of ransomware were identified in Q2 2015

Ransomware increased by **35%**

Ransomware found **new targets** in smart phones, Mac and Linux systems

In Q1 2016, the FBI estimated that **more than $209 million** had been lost to ransomware attacks



Any Organization Can be a Target

Mitigate the Risk of Ransomware

With new variants proliferating at a rapid pace, security measures cannot focus solely on prevention. For example, removing local administrator rights can sometimes prevent ransomware from executing, but not all types of ransomware require admin rights. Organizations must assume some ransomware will enter their networks and mitigate risks accordingly.

CyberArk Viewfinity takes a unique approach to protecting an organization from the damaging effects of ransomware with a combination of least privilege and application control. The solution greylists unknown applications and enables them to run in Restricted Mode to limit the resources they can reach. This enables organizations to protect themselves from both known and unknown threats.

- Block access to internet, so ransomware can't make a call back to the master server run by the attacker
- Block access to corporate drives, so ransomware can't access/alter/encrypt shared files
- Block access to local files, so ransomware can't alter or encrypt files

This approach is signature-less and will protect against new flavors and variants of ransomware. By applying a layer of security around the operation of unknown applications, the solution is not limited to specific types of known malware or ransomware that is attempting to cause damage.

For more information, visit **www.CyberArk.com/Viewfinity**

Sources:
http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/
http://www.slideshare.net/AndyThompson11/ransomware-history-analysis-mitigation-pdf
http://www.securitymagazine.com/articles/86787-ransomware-attacks-to-grow-in-2016
https://www.symantec.com/security-center/threat-report
http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

CYBERARK