Improving Cyber Defensive Postures | Breaches are Certain, Impact is Not

April 20, 2017

Ken Liao, Vice President of Product Marketing
Who Am I?

Ken Liao, Vice President Product Marketing

Over 10 years of InfoSec industry experience

Helping businesses, schools, and government agencies protect their endpoints
Why Malwarebytes?

De facto STANDARD for remediation—you may be using Malwarebytes today!
Why Malwarebytes?

Human Approach

Machine Approach

Trusted by MILLIONS

De facto STANDARD for remediation—you may be using Malwarebytes today!
Responding to Breaches

DETECTION
CONFIRMATION
INVESTIGATION
RESPONSE

MAINTAIN PERSISTENCE
USE STOLEN CREDENTIALS TO RE-ENTER / FORTIFY ADDITIONAL ENTRY POINTS
EXECUTE MALICIOUS ACTIVITY
EXFILTRATE DATA

RECON ENTERPRISE RESOURCES
MOVE LATERALLY
EXECUTE APPROACH TO CIRCUMVENT DEFENSES

EXTRAS
ASSISTING ATTACKER IN MAPPING THE ENTERPRISE LANDSCAPE
EXPOSING INTERNAL & EXTERNAL CREDENTIALS
DEGRADING ENDPOINT PERFORMANCE

End of Attacker Window

USER://

Successful Breach

Incident Alert

DETECTION
CONFIRMATION
INVESTIGATION
RESPONSE
Responding to Breaches

**Detection**
- RECON ENTERPRISE RESOURCES
- USE STOLEN CREDENTIALS TO RE-ENTER / FORTIFY ADDITIONAL ENTRY POINTS
- EXECUTE MALICIOUS ACTIVITY
- EXFILTRATE DATA
- ENUMERATE VULNERABLE HOSTS
- PIVOT TO ADDITIONAL COMPROMISED HOSTS
- ESCALATE PRIVILEGES
- MOVE LATERALLY

**Confirmation**
- COMPROMISE CREDENTIALS
- C&C
- EXPOSING INTERNAL & EXTERNAL CREDENTIALS
- DEGRADING ENDPOINT PERFORMANCE
- ASSIST ATTACKER IN MAPPING THE ENTERPRISE LANDSCAPE
- SHARING ATTACK VERTICES WITH OTHER ENDPOINTS

**Investigation**
- MAINTAIN PERSISTENCE
- SUCCESSFUL BREACH
- END OF ATTACKER WINDOW
- INCIDENT ALERT

**Remediation**
- USER://
- BREACH
- RESPONSE
Breaking the Attack Chain

Pre-execution

Profiling → Delivery → Exploitation → Payload Execution → Malicious Behavior

Post-execution
Breaking the Attack Chain

Pre-execution

Profiling

Delivery → Exploitation → Payload Execution → Malicious Behavior

Post-execution

• **Application hardening** reduces vulnerability surface and proactively detects fingerprinting attempts used by advanced attacks.
  (Signature-less)
Breaking the Attack Chain

**Pre-execution**
- Profiling
- Delivery
- Exploitation
- Payload Execution
- Malicious Behavior

**Post-execution**

- **Web protection** prevents access to malicious websites, ad networks, scammer networks, and bad neighborhoods.
Breaking the Attack Chain

- **Exploit mitigations**: proactively detect and block attempts to abuse vulnerabilities and remotely execute code on machine. (Signature-less)

- **Application behavior protection**: prevents apps from infecting the machine. (Signature-less)
• **Payload analysis** with heuristic and behavioral rules, identifies entire families of known and relevant malware.

• **Machine learning** (in beta) proactively identifies viruses and malware. (Signature-less)
Breaking the Attack Chain

Pre-execution

Profiling → Delivery → Exploitation → Payload Execution

Post-execution

Malicious Behavior

- **Ransomware mitigation** detects and blocks ransomware via behavior monitoring technology. (Signature-less)
- **Callback protection** prevents access to C&C servers and other malicious websites.
- **Incident response** engine quickly and thoroughly removes infection and all artifacts. (Signature-based & signature-less)
Breaking the Attack Chain
Thank you

Learn More: malwarebytes.com

Latest News: blog.malwarebytes.com

Request a Trial: malwarebytes.com/business/licensing

Follow Us: Facebook, Twitter, LinkedIn, YouTube