# Polymorphic and Metaphoric Threats and Your Cyber Future

## RSA FirstWatch
## Advanced Threat Research and Intelligence

Will Gragido, Sr. Manager RSA First Watch
William.gragido@rsa.com
Christopher Elisan, Principal Malware Researcher
Chrisptopher.Elisan@rsa.com

2012

# Agenda

- About Us
- The rise of polymorphism and metamorphism
- Their role in sophisticated / advanced attacks
- What can be done if you encounter these threats
- Questions and Answers

# RSA FirstWatch

## Advanced Threat Research & Intelligence

- Established in April 2012
- Mission:
- To provide RSA NetWitness customers covert tactical and strategic threat intelligence on advanced threats & actors
- Elite, highly trained threat research & intelligence team
  - Recent Works

    VOHO Advanced Persistent Threat Campaign

    Kneber Zeus

# The Rise of Polymorphism and Metamorphism

## Polymorphism

- Code that uses a polymorphic engine to mutate while keeping the algorithm intact
- Code cannot rewrite itself
- Obfuscates the encryption/decryption engine to avoid identification of the malware using this element of the malware encryption process
- Common methods:
  - Encryption
  - Appending data or Pre-pending data
- First known example of malicious code of this type:
  - 1260 written in 1990
- Virut is a well known example but it's old … we're here to talk about new stuff!

# The Rise of Polymorphism and Metamorphism

## Metamorphism

- Code that can mutate itself without sacrificing functionality
- Differs greatly from polymorphism
  - Polymorphs are similar in memory while metamorphs are not
  - Polymorphs still uses traditional malware encryption elements while metamorphs do not
- Used by many malicious code samples during the infection of new files with the next generation looking nothing like the previous one
- Common methods:
  - Adding varying lengths of NOP instructions
  - Permuting use registers
  - Adding useless instructions and loops within the code segments Metamorphic segments
  - Replacing lines of codes with different instructions but with similar result (e.g. MOV AX, 0 and XOR AX, AX)
- Examples:
  - Zmist or Zombie.Mistfall 2001
  - Simile written in 2002

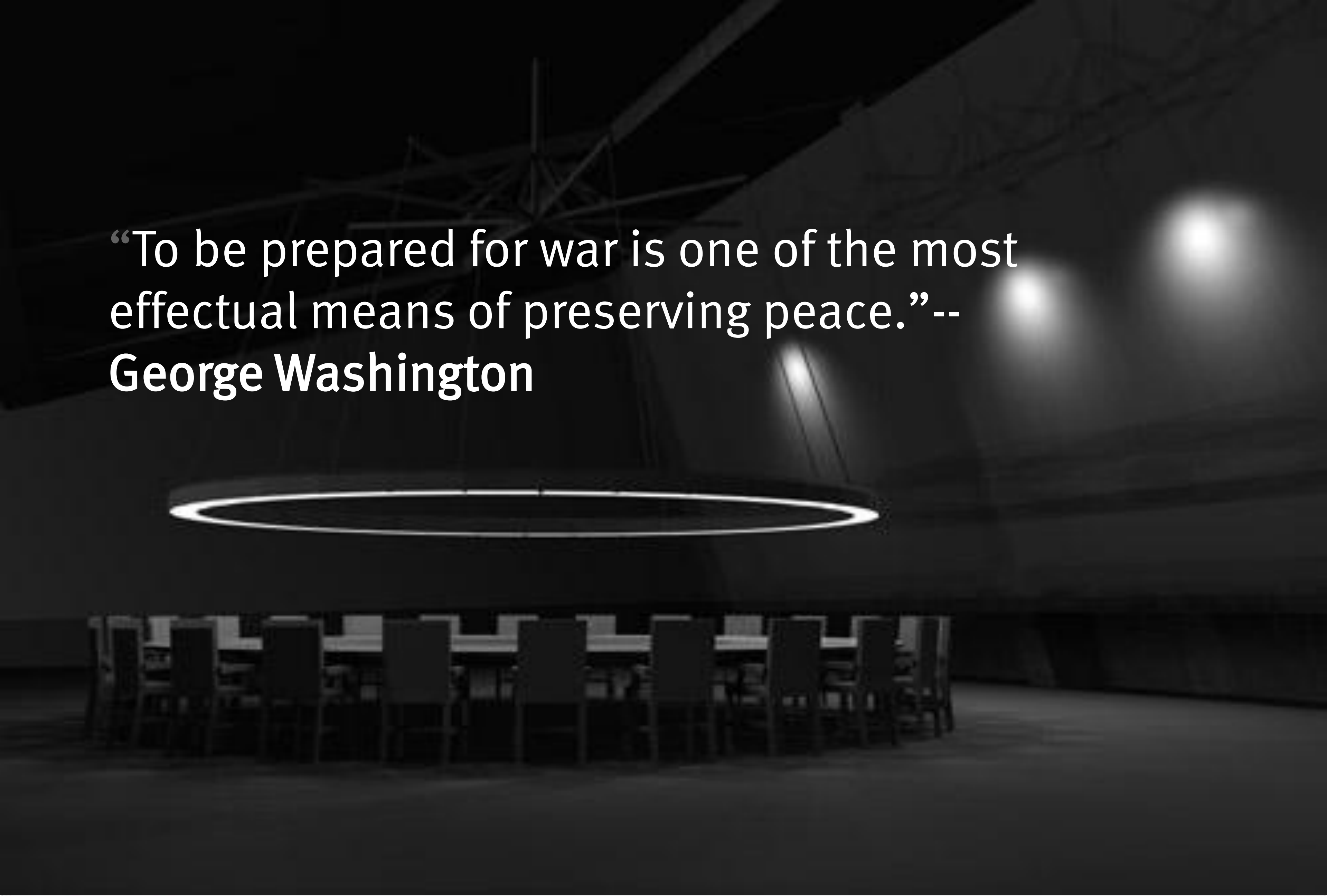
# The Rise of Polymorphism and Metamorphism

## Their role in advanced / sophisticated attacks

- The truth is in the modern threat landscape…
- You don't see too many examples of advanced / sophisticated attacks using polymorphism or metamorphism
- Were we to see a rise of these in modern attacks it would surely represent challenges and headaches for the industry such as in the heyday of the virus' earliest days
- There are some examples that are *similar* to polymorphic code but they don't fit the definition entirely:
  - Zeus
  - SpyEye
  - Silon
  - Tilon

# What can be done to mitigate these threats

- Knowing what you are contending with is key
- Identification of code type is essential to defense, mitigation and remediation
  - Comprehensive establishment of IOCs
  - Execution of IOCs in lab environments for remediation
- Polymorphic code, when decrypted, is essentially the same in all cases as a result memory based signature detection is possible
- Metamorphic code, are totally different on disk and in memory making traditional signature based detection uselsss



"To be prepared for war is one of the most effectual means of preserving peace."--
George Washington

# THANK YOU

rsafirstwatch@rsa.com