NIC

2019

Artificial Edition

6-8 February

Modern Malware:
Leveraging Its Imperfection to Design Response Methods

Paula Januszkiewicz

CQURE: CEO, Penetration Tester / Security Expert
CQURE Academy: Trainer
MVP: Enterprise Security, MCT
MS: Regional Director
Contact: paula@cqure.us | http://cqure.us
Security videos: http://cqureacademy.com

CQURE

@paulacqure
@CQUREAcademy

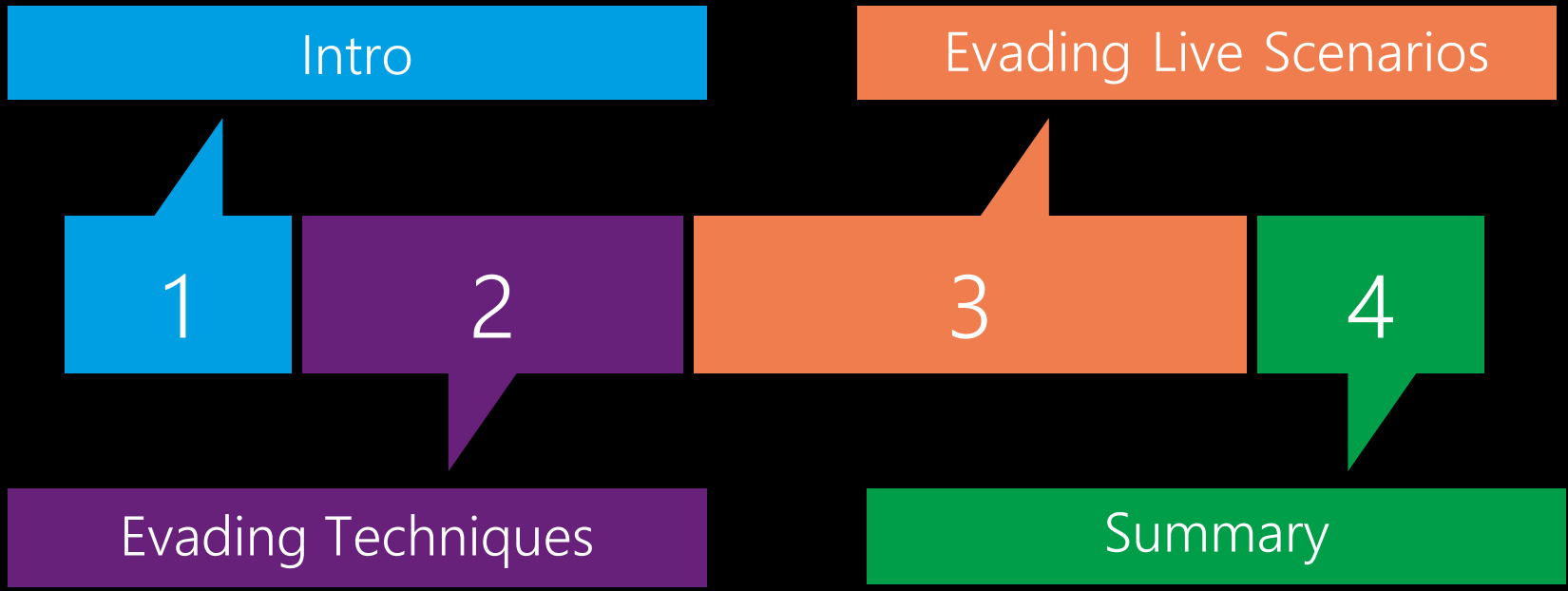

Featured TechEd 2012 Speakers
More featured speakers →
Wally Mead
John Craddock
Mark Russinovich
Paula Januszkiewicz


RSAConference2017
CQURE
RSAConference 2017
San Francisco | February 13–17 | Moscone Center


DPAPI AND DPAPI-NG:
DECRYPTION TOOLKIT
PRESENTED BY: Paula Januszkiewicz
Business Hall, Arsenal Station 3
December 6 | 1:30pm-3:05pm
CQURE
black hat
EUROPE 2017


Microsoft
CQURE ACADEMY©
We are proud to announce that
Paula Januszkiewicz
was rated as
No 1 Speaker
at Microsoft Ignite!!!
May 4-8, 2015
Chicago, IL

Agenda


Intro
Evading Live Scenarios
1
2
3
4
Evading Techniques
Summary


We have the best security solutions...


...but the security landscape has changed.

Demo: SDDL - Can antivirus be stopped?

Techniques for malware discovery

Behavior-based

Attempts to open, view, delete, and/or modify files.

Attempts to format disk drives and other unrecoverable disk operations.

Modifications to the logic of executable files, scripts of macros.

Signature-based

Can rely on the imphash" (uses library/API names and their specific order within the executable).

Modification of critical system settings, such as start-up settings.

Scripting of e-mail and instant messaging clients to send executable content.

Initiation of network communications.

1- Evasion Techniques Used by Malware

Packers and Encryptors

Tools used to compress and encode binary files. Packer will "unpack" the payload into memory and execute it.

Tools and techniques: UPX, PECompact, Armadillo, Encoders (Metasploit), Hyperion

Wrapping

Attaches the malicious payload (the installer or the malware itself) to a legitimate file.

Demo: Hyperion

2- Evasion Techniques Used by Malware

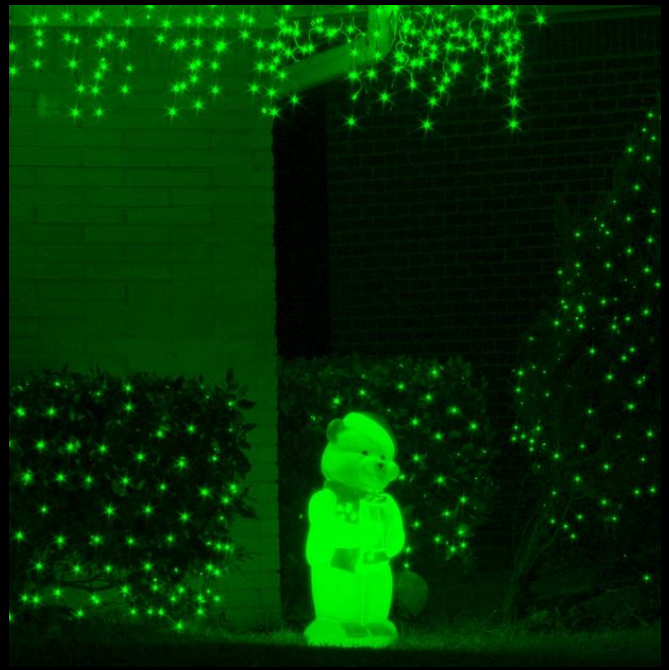
Obfuscation

Modifies high level or binary code it in a way that does not affect its functionality, but changes its signature.

Anti-debugging

Prevents a binary from being analyzed in an emulated environments such security sandbox etc.

Examples: ZeroAccess, sleep function



Reflective PE Loader

Custom code

User Mode Loaders

Executable is extracted and decrypted in memory

Code is loaded and executed dynamically

In Powershell.exe – not every module is embedded – they can be created and loaded during the execution

In Win32API: Custom code mimics LoadLibrary()

Interesting: During the compilation, that's what helps us:

```
CompilerParameters.CompilerOptions =
"/platform:x64";
```

Demo: Custom Reflective PE Loader - CQPELoader

3- Evasion Techniques Used by Malware

Targeting

Used to:

Attack a specific part of a system (IE, Firefox etc.), and act as one (Create Remote Thread etc.)

Detect specific settings (VMWare, Process Explorer running etc.) to prevent analysis.

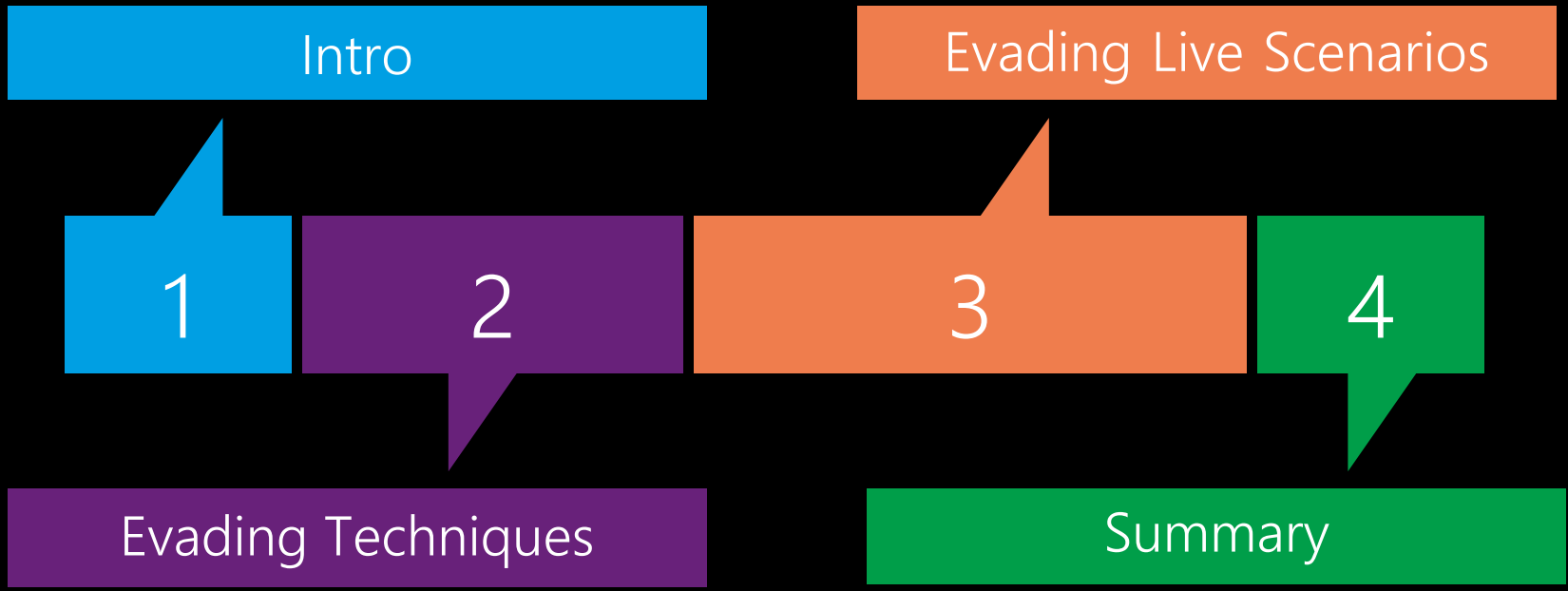
Typical examples are:

Do not run if network card is Microsoft Corporation

Do not run if wireshark.exe is working

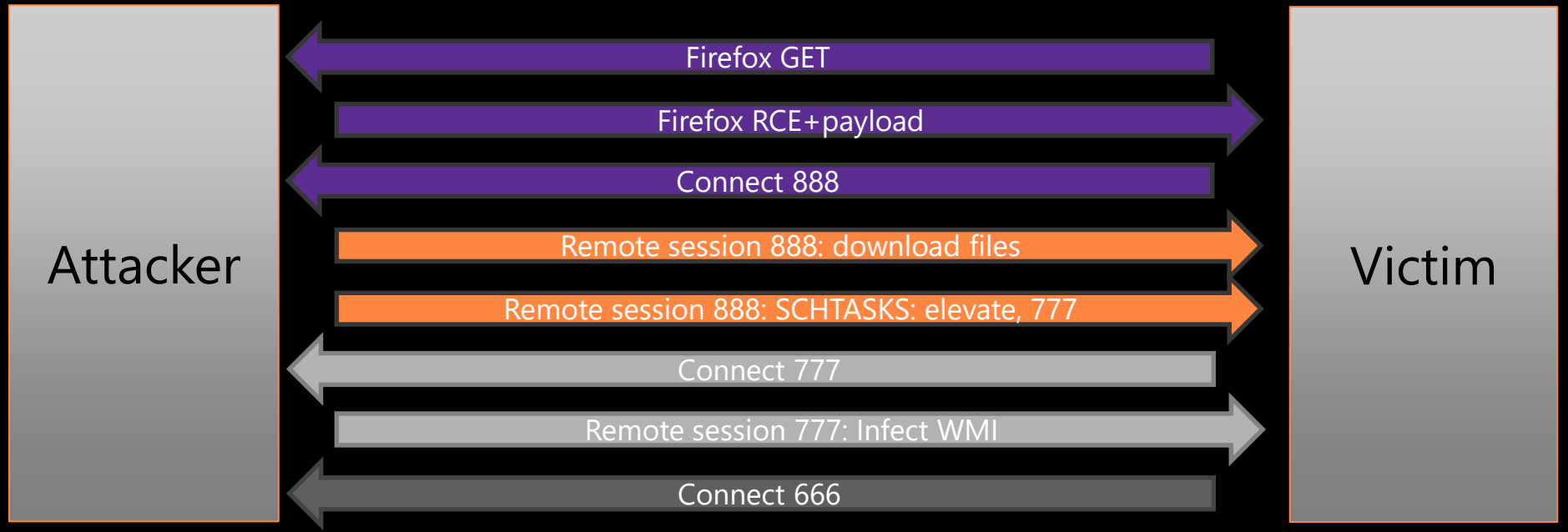
Do not run if windbg.exe is running

Agenda


Intro
Evading Live Scenarios
1
2
3
4
Evading Techniques
Summary

Demo: Evasion Scenario

Scenario:


Attacker
Firefox GET
Firefox RCE+payload
Connect 888
Remote session 888: download files
Remote session 888: SCHTASKS: elevate, 777
Connect 777
Remote session 777: Infect WMI
Connect 666
Victim

Scenario 1: Techniques used

1. Attacker uses exploitable bug in the Firefox to remotely execute the code
2. Attacker uses the bug in Windows (MS16-032) to elevate from user to the Local System account
3. Attacker injects the script to the WMI repository

Scenario 2: Techniques used

1. Intro: Script in the WMI Repository
2. It writes a file into the disc (source code
3. Source code is compiled to executable (EXE)
4. EXE is executed and it finds svchost.exe
5. EXE injects a payload into the svchost.exe
6. EXE calls CreateRemoteThread in svchost.exe to run a custom remote shell

Demo: Execution through the debugger

AMSI

Antimalware Scan Interface (AMSI)

It is a generic interface standard that allows applications and services to integrate with any antimalware product

Techniques used

It supports a calling structure allowing for file and memory or stream scanning, content source URL/IP reputation checks, and other techniques

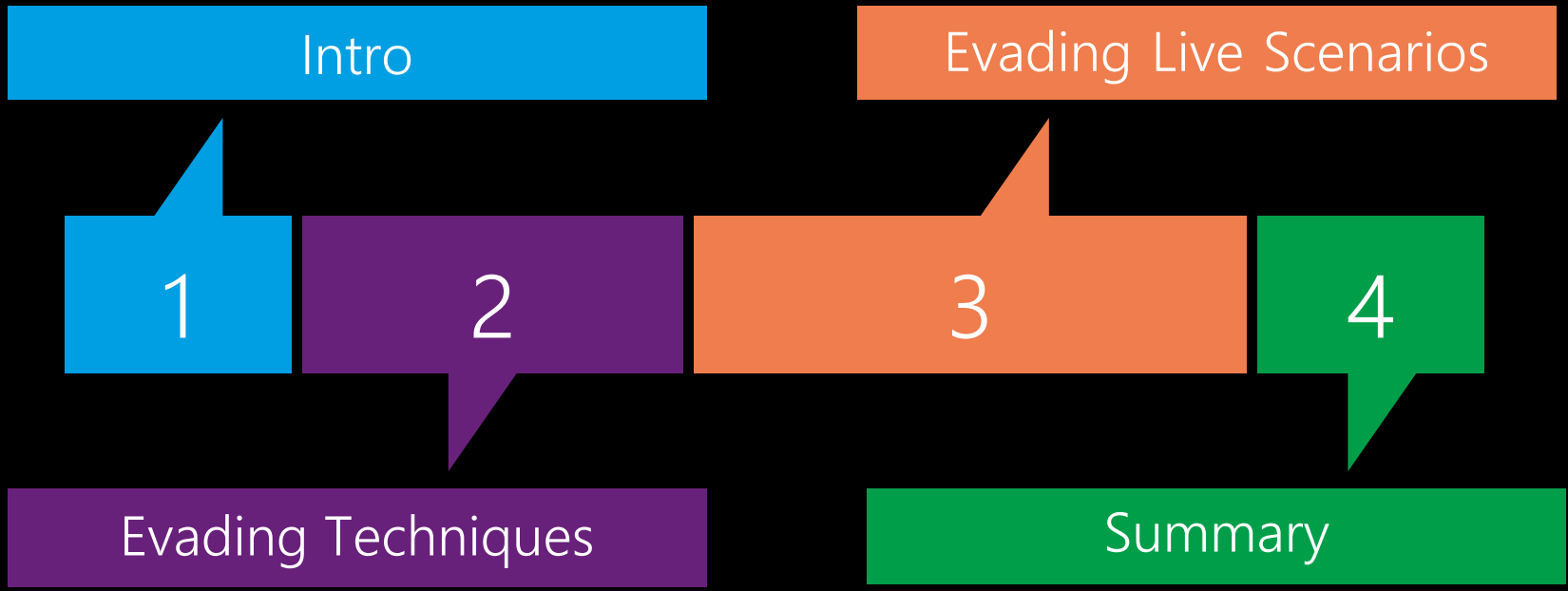
Allows correlation of events

The different fragments of a malicious payload can be associated to reach a more informed decision, which would be much harder to reach just by looking at those fragments in isolation.

Demo: AMSI in action

Demo: Sysmon

Agenda


Intro
Evading Live Scenarios
1
2
3
4
Evading Techniques
Summary

Summary: Bypassing techniques and mitigations

1. The only cure is a **_complete_** code execution prevention
2. Anti-Exploit solutions make a lot of sense
3. Sysmon (absolutely!)
4. At the end it is a matter of budged and price
5. Code execution prevention solutions are often misconfigured

Thank you!

Modern Malware:
Leveraging Its Imperfection to Design Response Methods

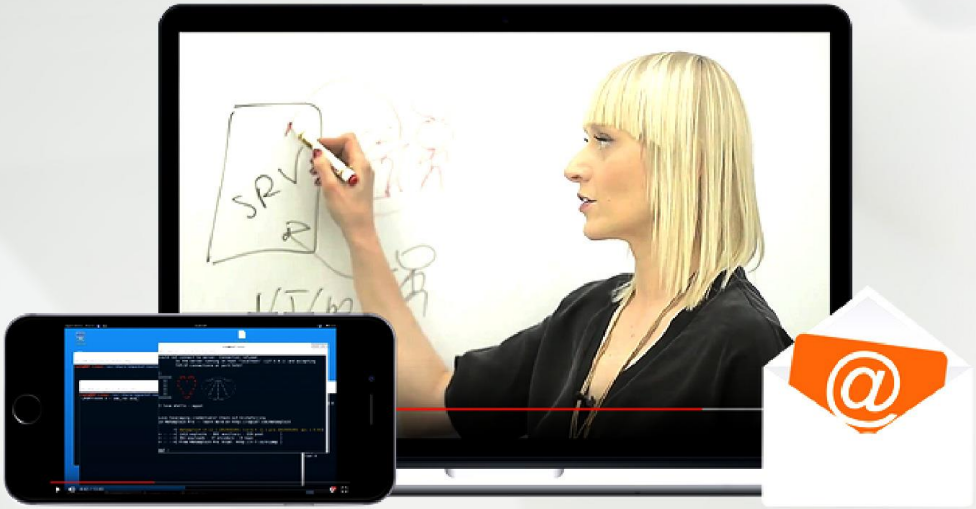
Paula Januszkiewicz

CQURE: CEO, Penetration Tester / Security Expert
CQURE Academy: Trainer
MVP: Enterprise Security, MCT
MS: Regional Director
Contact: paula@cqure.us | http://cqure.us
Security videos: http://cqureacademy.com

CQURE

@paulacqure
@CQUREAcademy

To get **SLIDES & TOOLS** (and not to miss out on my WEEKLY video tutorials):



Sign up for our weekly newsletter
Cqureacademy.com/newsletter

Like CQURE Academy on Facebook:
Facebook.com/CQURE

Follow me on Twitter:
@PaulaCqure

(The best option - all of the above! I won't think you're a stalker, promise.)