nic

2019

Artificial Edition

6-8 February

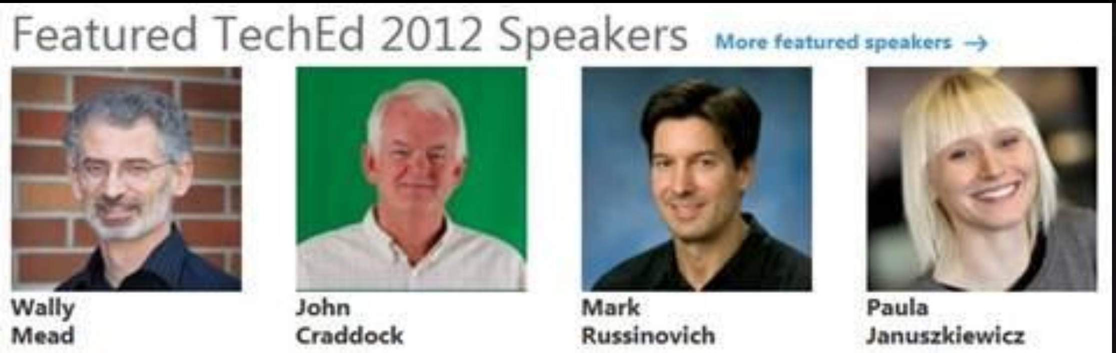
Fatal signs: 10 symptoms when you think you've been hacked

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

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

Session Abstract

We all need the mandatory list of places to check in case of being hacked, or at least when we are in doubt. There are OS behaviors that could indicate something is currently active, but how can we spot exactly what that is? We look at the places used by the system to store such information.

Surprisingly, your disk drive contains a lot of juicy information that can reveal secrets and history. There are also places where data can be deliberately hidden by malicious software and it would be great to know where! Become familiar with the symptoms that could indicate you have been hacked, and tools and techniques to spot these kind of activities. Also, learn how you can mitigate hackers to exploit discussed OS areas.

AM
PM
LA:TE
ALARM
FM 88 92 96 100 104 108 MHz
FM/AM CLOCK RADIO
AM 53 60 70 80 100 130 170 x10kHz

#1 Network traffic anomalies

#2 Performance issues on DNS / Unusual processes communicating over network

#3 Unexpected service behavior / Unusual Prefetch content

#4 System files with different hashes on different computers

#5 Change of group membership or privileges

#6 Usage of seDebugPrivilege

#7 Watchdog files -> touched

#8 SCRCONS – WMI Modification

#9 Patterns in Sysmon

#10 Suspicious deleted files

10 fatal signs

#1 Network traffic anomalies

#2 Performance issues on DNS / Proceses communicating over network

#3 Unexpected service behavior / Unusual Prefetch content

#4 System files with different hashes

#5 Change of group membership or privileges

#6 Usage of seDebugPrivilege

#7 Watchdog files -> touched

#8 SCRCONS – WMI Modification

#9 Patterns in Sysmon

#10 Suspicious deleted Files

Session summary

Continuous activities

- Review configuration of servers' and workstations' periodically

Prevention

- Act proactively: **Implement code execution prevention and exploit prevention** solutions
- Reconsider **privileged access management**
- **Isolate infrastructure components** so that in case of attack they prevent spreading

Analysis

- Investigate and remediate unknown traffic

Thank you!

Fatal signs: 10 symptoms when you think you've been hacked

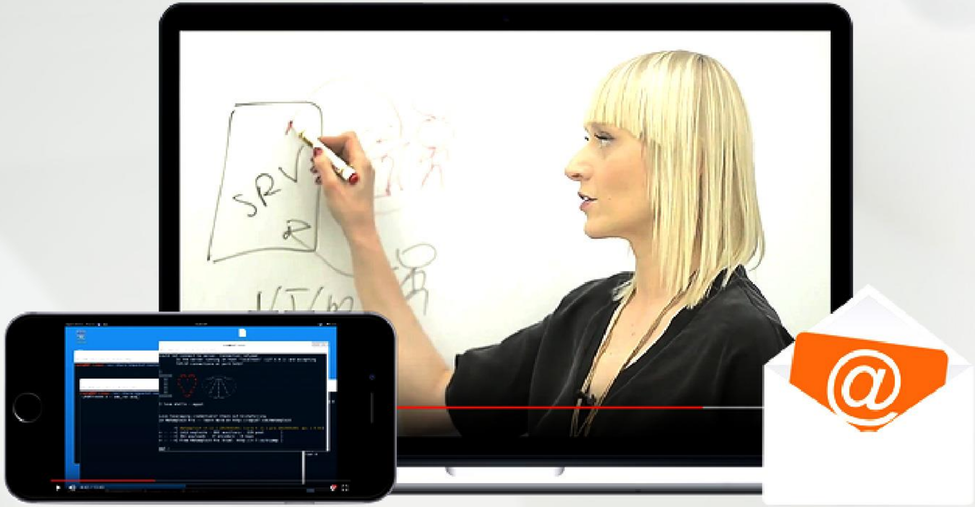
Paula Januszkiewicz

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.)