RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

BETTER.

SESSION ID: FLE R02

Fatal signs: 10 Symptoms When You Think You've Been Hacked

Paula Januszkiewicz

CQURE: CEO, Penetration Tester; Security Expert
CQURE Academy: Trainer
MS MVP: Cloud and Datacenter Management, MCT
Microsoft Regional Director
www.cqureacademy.com
paula@cqure.us

RSAConference2019
Asia Pacific & Japan

What does CQURE Team do?

Consulting services

- ✓ **High quality penetration tests** with useful reports
  - Applications
  - Websites
  - External services (edge)
  - Internal services

  + configuration reviews
- ✓ **Incident response** emergency services – immediate reaction!
- ✓ **Security architecture and design advisory**
- ✓ **Forensics investigation**
- ✓ **Security awareness**

  For management and employees

Trainings

- ✓ **Security Awareness trainings** for executives
- ✓ **CQURE Academy:** over 40 advanced security trainings for IT Teams
- ✓ **Certificates and exams**
- ✓ **Delivered all around the world only by a CQURE Team**: training authors

info@cqure.us

Featured TechEd 2012 Speakers

More featured speakers →

Wally Mead

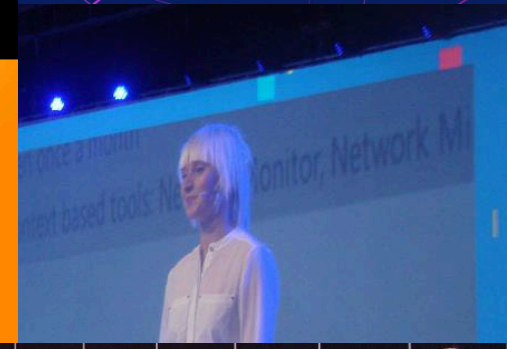
John Craddock

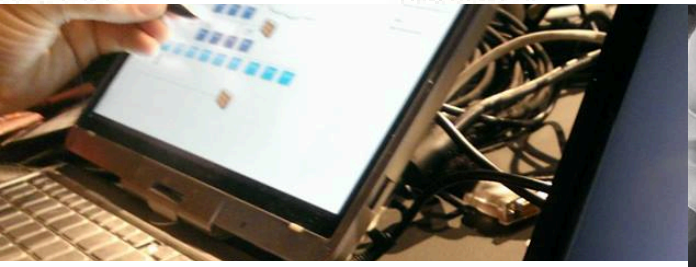
Mark Russinovich

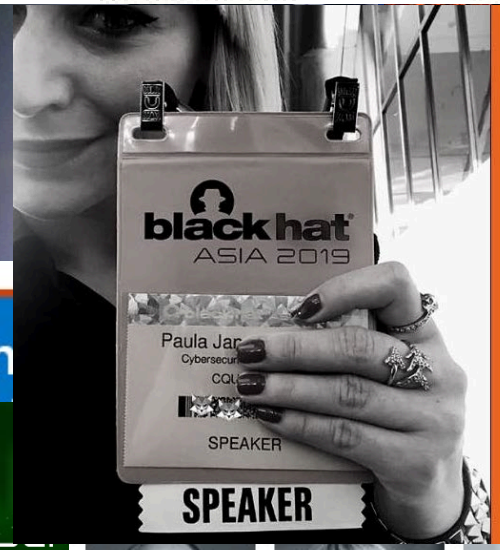
Paula Januszkiewicz

Microsoft CQURE ACADEMY©

We are proud to announce that
Paula Januszkiewicz
was rated as
No 1 Speaker
at Microsoft **Ignite!!!**







No.1 Speaker

Paula Januszkiewicz
CEO CQURE

She received
a **"Best of Briefings"** award at her
"CQTools: The New Ultimate Hacking Toolkit"
Black Hat Asia 2019 briefing session

black hat

TechEd Learn. Con

black hat USA 2017

ATTEND | TRAININGS | BRIEFINGS | ARSENAL | FEATURES | SCHEDULE | SPECIAL EVE

SEE ALL PRESENTERS

SPEAKER

PAULA JANUSZKIEWICZ
COURE INC.

Paula Januszkiewicz is a CEO and Found
also an Enterprise Security MVP and a wo
Customers all around the world. She has
deep belief that positive thinking is key
extreme attention to details and confere

Brian Keller

Paula Januszkiewicz

Mark Minasi

John Craddock

Scott Woodgate

Marcus Murray

ccommodation | Agenda & Sessions | Sponsors | Contact Us

November 3

General Sessions | Applications and Development | Cryptography and Architecture | Hackers and Threats | Mobile and Network Security | Trusted and Cloud Computing

Mark Kennedy
Symantec
Topic: Anti-Malware Industry... Cooperating. Are You Serious?

Samir Saklikar
Dennis Moreau
RSA, The Security Division of EMC
Topic: Big Data Techniques for Faster Critical Incident Response

Marc Bown
Trustwave
Topic: APAC Data Compromise Trends

Paula Januszkiewicz
CQURE
Topic: Password Secrets Revealed! All You Want to Know but Are Afraid to Ask

RSAConference2019
Asia Pacific & Japan

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.

CONSULTING

What has evolved over the years?

During forensic take into consideration the new malware trends, e.g.:

- ✓ Malware tries to blend in day-to-day admin operations (PowerShell scripts, LOLBINS, etc.);
- ✓ Machine learning may be used to identify malicious activity but also it may be used to make malware harder to analyse (e.g. hard to analyze ML model built in malware trained to check if it runs on the victim machine).


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 Disc analysis -> anomalies

#2 Unusual processes communicating over network


There is pretty much always something you can find…

Searching for a Trace: Disk

- Profile, NTUSER
- Run dialog
- Most Recently Used (MRU), Management Console (MMC)
- Remote Desktop connections
- Prefetch files
- Recent documents
- Automatic Destinations (LNK)
- Security Log
- RDP Operational Log
- Application Logs
- Temporary Internet Files
- Deleted files – recoverable from the disk
- NTFS Structures
- Hiberfil.sys
- Memory dumps

#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

Searching for a Trace: Memory

Handles
Processes
Hidden Processes (ActiveProcessLinks)
Files that can be extracted
Threads
Modules
Registry
API Hooks
Services
UserAssist
Shellbags
ShimCache
Event Logs
Timeline

#7 Watchdog files -> touched

File Level Games

Extension change

Joining files

Alternative data streams

Embedding

Playing with the content

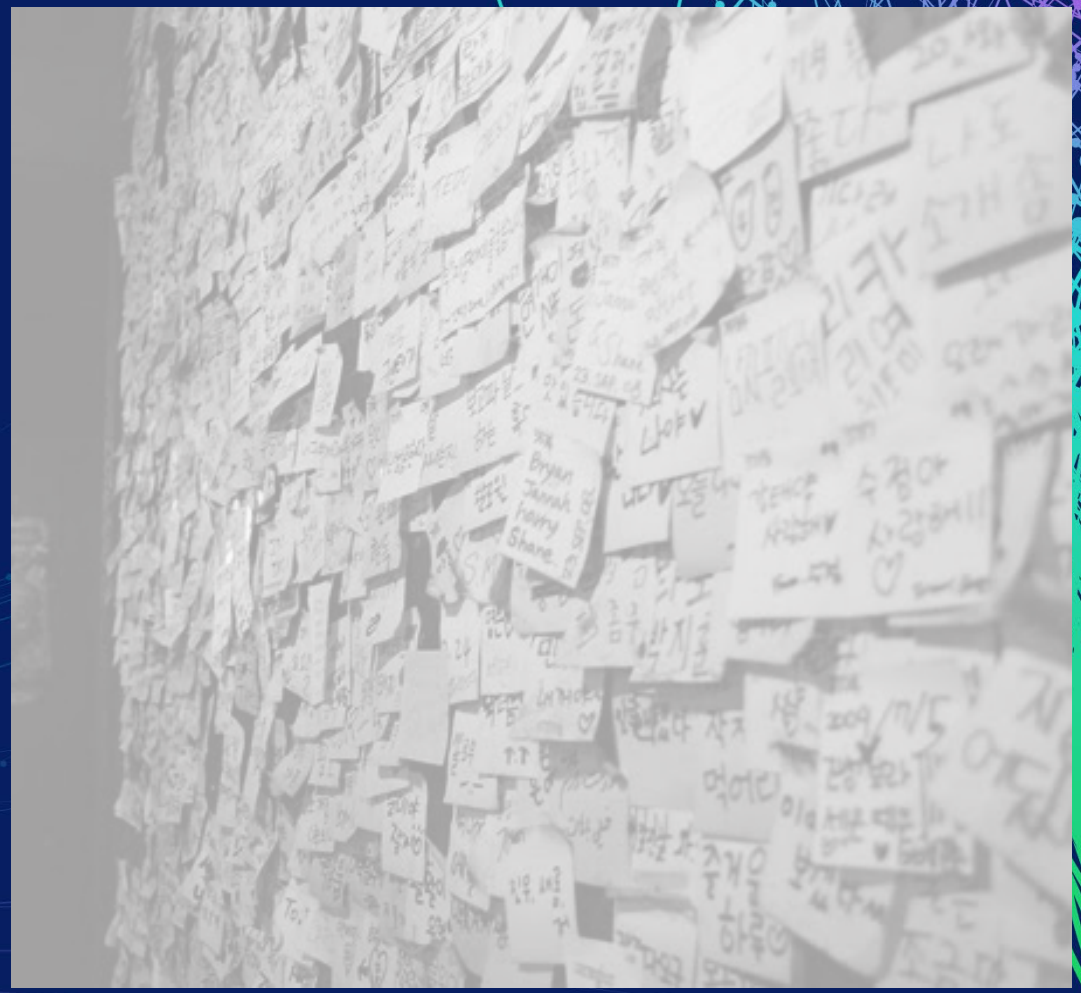
Steganography

Deletion

Disk Level Games

Hiding data

Encryption



#8 Social media activity / data revealed

#9 Patterns in Sysmon

#10 Suspicious deleted files

Entry Information

Allows to build an attack timeline

Allows to define an entry point and anomalies

Collects and records system events to the Windows event log

It is free and easy to set up

Good practices

Filter out uninteresting events (image loads etc.)

Make sure event log is big enough

Centralize the events in a separate server

You can download Sysmon from Sysinternals.com

RSAConference2019
Asia Pacific & Japan

#1 Disc analysis -> anomalies

#2 Unusual processes 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 Social media activity / data revealed

#9 Patterns in Sysmon

#10 Suspicious deleted Files

10 fatal signs

RSAConference2019
Asia Pacific & Japan

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

RSAConference2019
Asia Pacific & Japan

Thank you!

CQURE

To get SLIDES & TOOLS

(and not to miss out on my video tutorials):

Sign up for our 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

RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

BETTER.

SESSION ID: FLE R02

Fatal signs: 10 symptoms When You Think You've Been Hacked

Paula Januszkiewicz

CQURE: CEO, Penetration Tester; Security Expert
CQURE Academy: Trainer
MS MVP: Cloud and Datacenter Management, MCT
Microsoft Regional Director
www.cqureacademy.com
paula@cqure.us