



ITU Cyber Drill - ALERT (Applied Learning for Emergency Response Teams) for Europe Region

26-30 November 2018 | St Raphael resort, Limassol, Cyprus

Organized within the Framework of the ITU Regional Initiative for Europe on ICT-Centric Innovation Ecosystems



Hosted by

Digital Security Authority
of Cyprus





AGENDA

Sunday 25 November 2018

[19:00-21:00] **Welcome Drink organized by National CSIRT-CY**
Venue: St. Raphael Resort, Limassol

Monday 26 November 2018

FIRST TRAINING: Introduction to Reverse Engineering Malware

Introduction to Reverse Engineering Malware, will train Analysts, Incident Responders and Researchers to quickly dissect various malicious artifacts (executable, document, *script), triage the severity and extract indicators in a short amount of time. This workshop is designed for anyone who wants to start their journey into disassembling and debugging malicious binaries. Statically analyzing the artifacts helps in creating better detection and understanding the severity of the attack.

In this workshop we will learn how to extract and analyze malware found at different stages of an attack. We will walk through various tools used for debugging and disassembling such as OllyDbg, Ida, x64dbg etc. We will also look at reversing malware written in various languages such as C, .NET, Java, Autoit etc. The course will progress into identifying some advance tricks used by malware for anti-vm detection and anti-analysis.

Trainers: Mr Uttang Dawda and Mr Francesco Canestrelli

Course level: Intermediate

Pre-requisites: Understanding of Windows Internals and Operating System Familiarity with x86 and x86_64 assembly preferred

| | |
|------------------------|--|
| [8:30 – 9:00] | Registration |
| [9:00– 10:00] | Technical Training for CIRTs (FIRST) : Sandboxing |
| [10:00 – 10:30] | Coffee Break and Group Photo |
| [10:30 – 12:00] | Technical Training for CIRTs (FIRST): PE File format and Static Analysis |
| [12:00 – 13:30] | Lunch Break |
| [13:30 – 15:00] | Technical Training for CIRTs (FIRST): Analysing First Malware |
| [15:00 – 15:30] | Coffee Break |
| [15:30 – 17:00] | Technical Training for CIRTs (FIRST): Decompiling/Analyzing .NET binaries |



Tuesday 27 November 2018

| | |
|-----------------|---|
| [8:30 – 9:00] | Welcome Coffee |
| [9:00 – 10:00] | Technical Training for CIRTs (FIRST): Debugging with OllyDbg and x64dbg |
| [10:00 - 10:30] | Coffee Break and Group Photo |
| [10:30 – 12:00] | Technical Training for CIRTs (FIRST): Packers and Unpacking |
| [12:00 – 13:30] | Lunch Break |
| [13:30 – 15:00] | Technical Training for CIRTs (FIRST): Injection and Stealth Launchers |
| [15:00 – 15:30] | Coffee Break |
| [15:30 – 17:00] | Technical Training for CIRTs (FIRST): Anti-VM, Anti-Analysis techniques |

Wednesday 28 November 2018

| | |
|-----------------|---|
| [8:30 – 9:00] | Registration [for those not participating in earlier training] |
| [9:00–9:45] | <p>Opening Ceremony</p> <ul style="list-style-type: none"> Welcome Address by H.E. Ms Vassiliki Anastasiadou, Minister, Ministry of Transport, Communications and Works <p>Opening Addresses</p> <ul style="list-style-type: none"> Mr George Michaelides, Commissioner, Office of the Commissioner of Electronic Communications and Postal Regulations Mr Jaroslaw Ponder, Head of ITU Office for Europe, International Telecommunication Union Mr Nicos Nicolaides, Mayor of Limassol Mr Marios Thoma, Training Manager, European External Action Service |
| [9:45 – 10:05] | Coffee Break and Group Photo |
| [10:05 – 11:30] | <p>Session 1 : Cybersecurity in the Region</p> <p>Setting the Context and Moderation: Ms. Rosheen Awotar-Mauree, Programme Officer, ITU</p> <p>Panelists</p> <ul style="list-style-type: none"> Mr Ioannis Askoxylakis, Policy Officer, European Commission Ms Pranvera Kastrati, Senior Expert on Economic & Digital Connectivity, RCC Ms Franziska Klopfer, Project Coordinator, DCAF Mr Mihai Rotariu, Public & Media relations coordinator, CERT-RO, Romania Mr Jakob Bund, Global Cyber Security Capacity Center, University of Oxford, UK Mr Peter Versmissen, Partner Deloitte Belgium |



[11:30 – 12:30] Session 2 : National and regional Cyber Exercises as a way to achieve Cyber Resilience
Setting the Context and Moderation : Ms Natalia Spinu, Chief of Cyber Security Center CERT-GOV-MD, **Moldova**

Panelists

- Mr Jonathan Martin, Anomali, **Cyprus**
- Mr Alessio De Angelis, Cyber Security Manager, **Deloitte**
- Mr Csaba Virag, Head of Cyber Security Competence Center, **Cyber Services Plc**
- Mr George Nicolaou, Head of Research and Incident Response, **Silensec**

[12:30 – 13:30] Lunch Break

[13:30 – 15:00] Session 3 : Critical Infrastructure Protection
Setting the Context and Moderation : Mr Antonis Antoniadis, Head of Digital Security Authority of **Cyprus**

Panelists

- Ms Andrea Dufkova, CSIRT Relations Team Leader, **ENISA**
- Mr Georgios Liassas, Technical Security Advisor, **NETS, Denmark**
- Mr Rastislav Janota, Director, **SK-CERT, Slovakia**
- Mr Battista Cagnoni, Cybersecurity Consulting Engineer, Vectra, **Switzerland**
- Mr Almerindo Graziano, **European Cyber Security Organisation (ECISO)**

[15:00 – 15:30] Coffee Break

[15:30 – 17:20] Session 4: Emerging issues in Cybersecurity
Setting the Context and Moderation: Mr Marwan Ben Rached, Technical Officer Cybersecurity, **ITU**

Panelists

- Dr Nadher Al-Safwani, Cybersecurity Consultant, **Oman ITU Regional Centre of Excellence**
- Mr Uttang Dawda, **FIRST**
- Mr Bill Nikolopoulos, Senior Cybersecurity Consultant, **Check Point**
- Mr Tõnu Tammer, Head of CERT-EE, **Estonian Information System Authority**
- Mr David Belder, Chief Information Officer, **Verint**
- Mr Antonis Proimadis, Senior Cybersecurity Engineer, **Fortinet**

[17:20 – 17:30] Concluding Remarks

- Mr Jaroslaw Ponder, Head of ITU Office for Europe, **ITU**
- Mr Antonis Antoniadis, Head of Digital Security Authority of **Cyprus**



18:00 **SOCIAL EVENT organized by National CSIRT-CY**
Participants are warmly invited to join us at: Winery 'Ktima Gerolemo', Omodos
(RSVP to the link <https://csirt.cy/omodos-winery-trip/>
Registration Form Password: G3r0l3m05)

Thursday 29 November 2018

| | |
|-----------------|--|
| [9:00 – 10:00] | Team creation, registering team accounts to Cyber Range |
| [10:00– 10:30] | Scenario 1 - Cyber threat intelligence Mr Almerindo Graziano, CEO, Silensec |
| [10:30 – 11:00] | Coffee Break |
| [11:00 – 12:30] | Scenario 1 - Cyber threat intelligence [continued] Mr Almerindo Graziano, CEO, Silensec |
| [12:30 – 13:30] | Lunch Break |
| [13:30 – 15:30] | Scenario 2 - Credit card fraud Mr Marwan Ben Rached, Technical Officer Cybersecurity, ITU |
| [15:30 – 15:45] | Coffee Break |
| [15:45 – 17:15] | Scenario 3 - Crisis management simulation Mr Ortalda, Alessandro, Deloitte |

Friday 30 November 2018

| | |
|-----------------|---|
| [9:00– 11:00] | Scenario 4 – Malware analysis Dr Nadher Al-Safwani, Cybersecurity Consultant, Oman ITU Regional Centre of Excellence |
| [11:00 – 11:15] | Coffee Break |
| [11:15 – 13:00] | Scenario 5 - Ransomware Analysis Mr Csaba Virág , Director of International Affairs, CyberServices |
| [13:00 – 13:30] | Cyberdrill wrap up Mr Marwan Ben Rached, Technical Officer Cybersecurity, ITU |
| | Concluding Remarks |
| | <ul style="list-style-type: none"> Ms Rosheen Awotar-Mauree, Programme Officer, ITU Mr Andreas Iacovou, Analyst, CSIRT-CY |
| [13:30-14:30] | Lunch |

