
NIC
EMPOWER
November 13-15, Oslo Spektrum

Viktor Hedberg

Device Code Phishing – How to detect and prevent those nasty phishers..

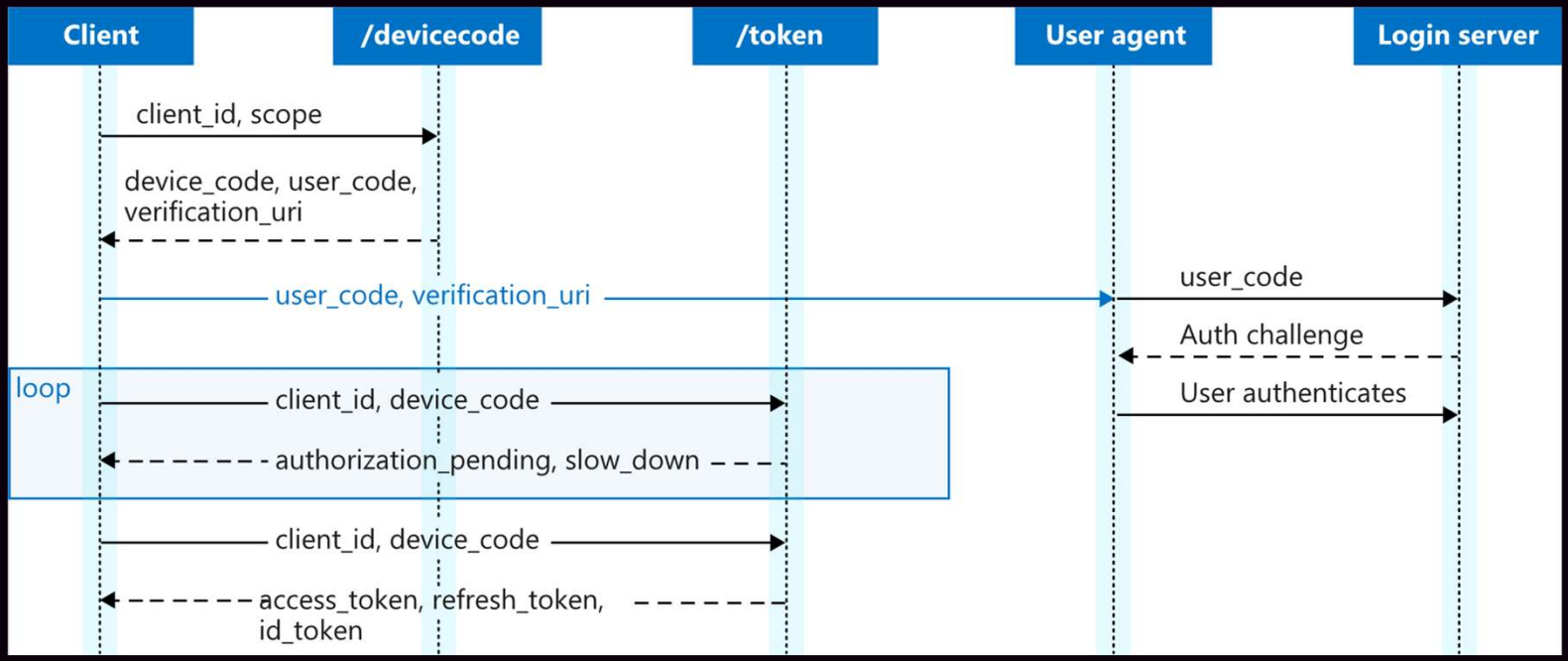
NIC
EMPOWER

/whoami

- Senior Technical Architect @ Truesec
- Works in the CSIRT
- Security Research (MS Cloud and On-Premises)

NIC
EMPOWER

Device Code Auth Flow



NIC
EMPOWER

Fear the FOCI

- Family of Client IDs:
- [family-of-client-ids-research/known-foci-clients.csv at main · secureworks/family-of-client-ids-research · GitHub]

NIC
EMPOWER

Constructing the “payload”

- Select which Graph Endpoint you wish to target
- Select a delivery method of the “payload”
- Select a FOCI app to leverage
- ... wait

DEMO

Constructing the payload and phish a user

NIC
EMPOWER

We´ve gotten the token!

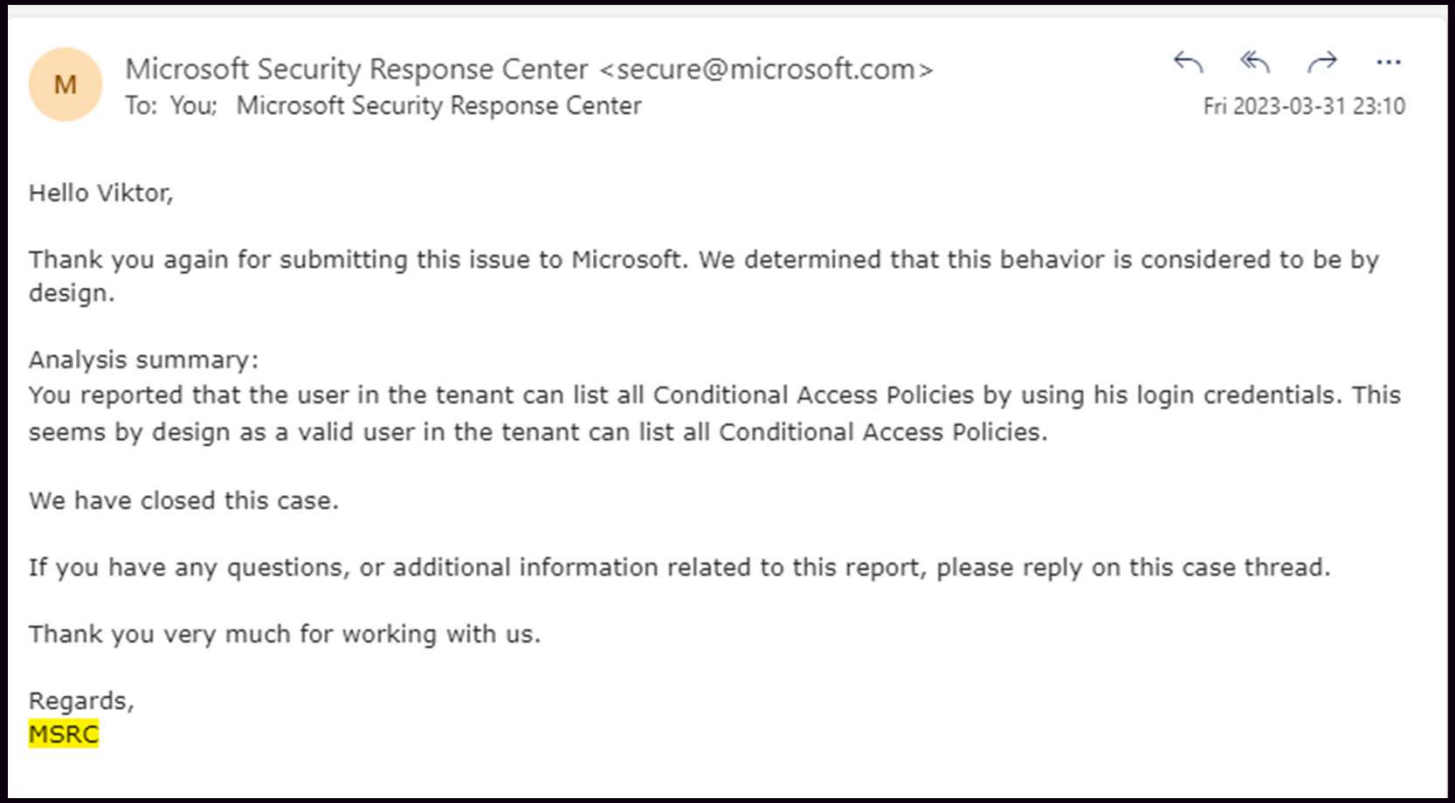
- What can we do with a token?
  - AADGraph = Lots
  - MSGraph = Eh, just as much as the user..
- So let´s play with AADGraph

DEMO

Playing with Access Tokens for AADGraph

NIC
EMPOWER

MSRC Response on the CA “vuln”



M

Microsoft Security Response Center <secure@microsoft.com>
To: You; Microsoft Security Response Center

Fri 2023-03-31 23:10

Hello Viktor,

Thank you again for submitting this issue to Microsoft. We determined that this behavior is considered to be by design.

Analysis summary:
You reported that the user in the tenant can list all Conditional Access Policies by using his login credentials. This seems by design as a valid user in the tenant can list all Conditional Access Policies.

We have closed this case.

If you have any questions, or additional information related to this report, please reply on this case thread.

Thank you very much for working with us.

Regards,
MSRC

NIC
EMPOWER

Detections.... Please?

- We can see it in the sign-in log.
- Yes, advanced hunting on CMSI:Cmsi will catch the Device code flow sign-in.

DEMO

Detections

NIC
EMPOWER

Prevention

- Conditional Access for Device code flow
- But how about the other stuff with AADGraph...?

DEMO

Conditional Access

NIC
EMPOWER

Prevention

- Conditional Access for Device code flow
- But how about the other stuff with AADGraph...?

- Sadly... We can only do “so” much until AADGraph ACTUALLY dies.
- Register the FOCI app to your Entra ID tenant.
  - Allows for Controlling who can connect to MSOL, AzureAD, AADGraph via that FOCI

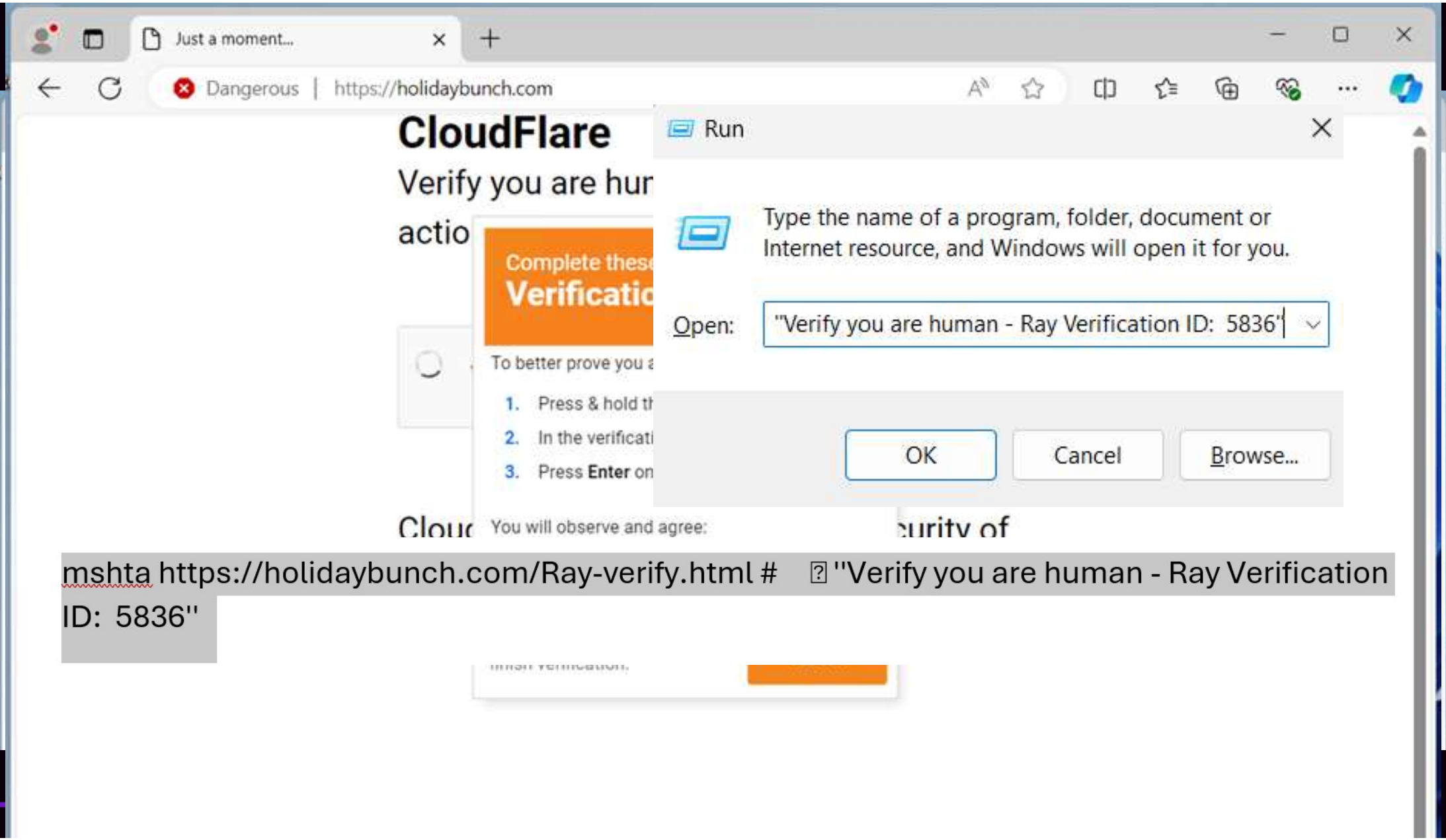
DEMO

Registered Azure Active Directory PowerShell

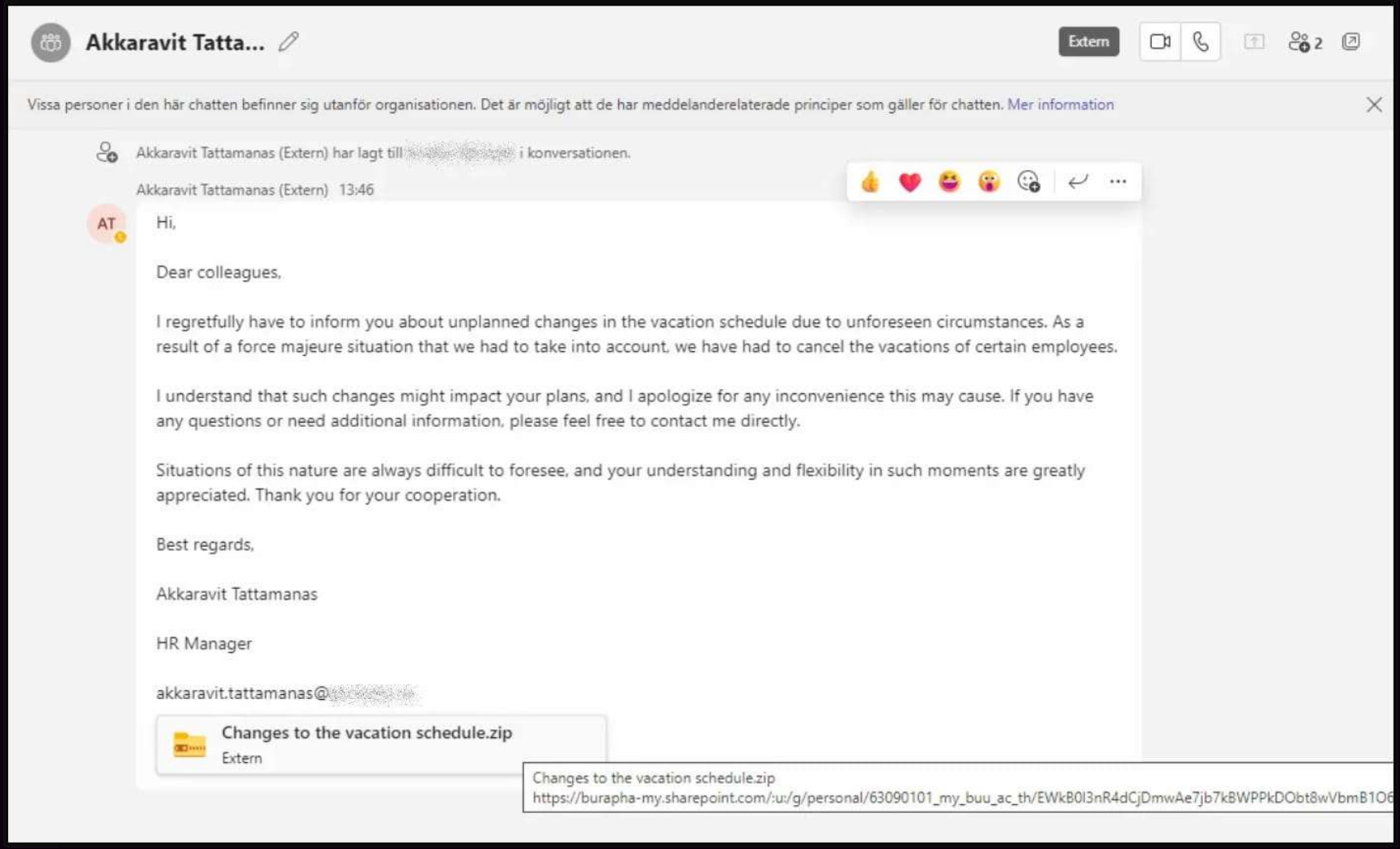
NIC
EMPOWER

Other “wierd” and cool phish’s

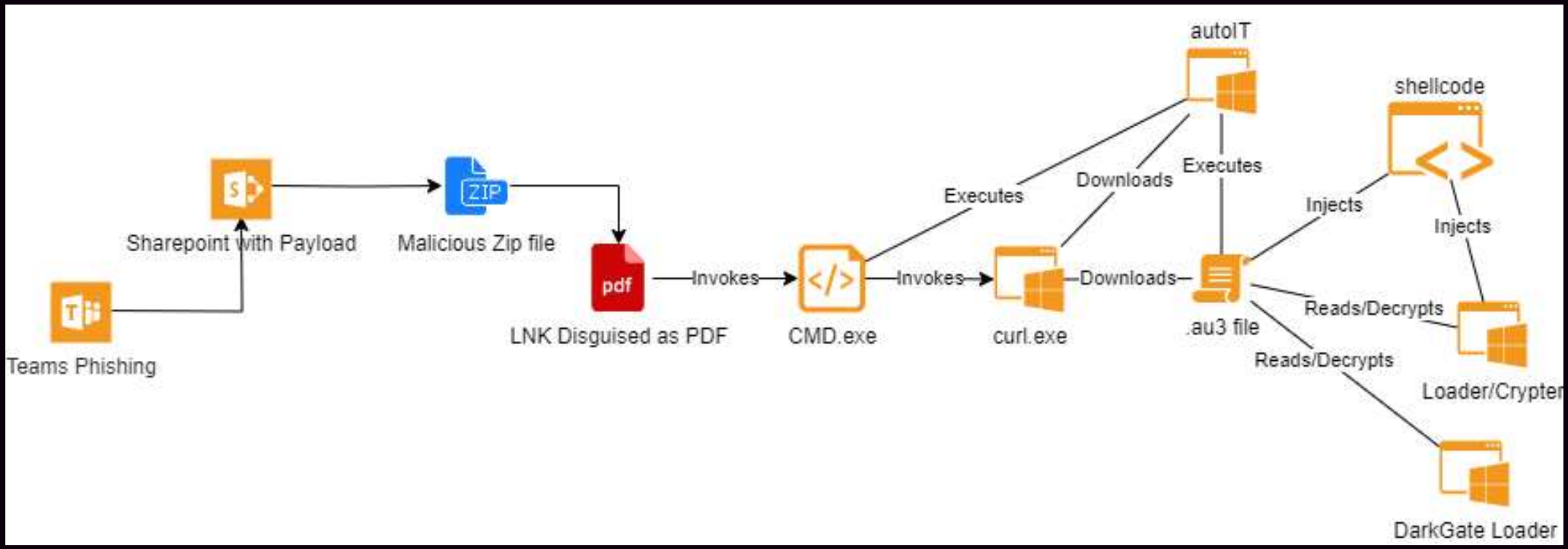
NIC
EMPOWER



mshta https://holidaybunch.com/Ray-verify.html # "Verify you are human - Ray Verification ID: 5836"


Akkaravit Tatta...
Extern
2
Vissa personer i den här chatten befinner sig utanför organisationen. Det är möjligt att de har meddelanderelaterade principer som gäller för chatten. Mer information
Akkaravit Tattamanas (Extern) har lagt till i konversationen.
Akkaravit Tattamanas (Extern) 13:46
AT
Hi,
Dear colleagues,
I regretfully have to inform you about unplanned changes in the vacation schedule due to unforeseen circumstances. As a result of a force majeure situation that we had to take into account, we have had to cancel the vacations of certain employees.
I understand that such changes might impact your plans, and I apologize for any inconvenience this may cause. If you have any questions or need additional information, please feel free to contact me directly.
Situations of this nature are always difficult to foresee, and your understanding and flexibility in such moments are greatly appreciated. Thank you for your cooperation.
Best regards,
Akkaravit Tattamanas
HR Manager
akkaravit.tattamanas@
Changes to the vacation schedule.zip
Extern
Changes to the vacation schedule.zip
https://burapha-my.sharepoint.com/:u:/g/personal/63090101_my_buu_ac_th/EWkB0l3nR4dCjDmwAe7jb7kBWPPkDObt8wVbmB1O6

NIC
EMPOWER


autoIT
shellcode
Executes
Downloads
Executes
Injects
Injects
Sharepoint with Payload
Malicious Zip file
pdf
Invokes
Invokes
Downloads
Reads/Decrypts
Reads/Decrypts
Teams Phishing
LNK Disguised as PDF
CMD.exe
curl.exe
.au3 file
Loader/Crypter
DarkGate Loader

NIC
EMPOWER

Summary

- Targeting Teams messages instead of traditional email.
- No safe links scan in this world will block it.
  - Because we´re leveraging MS Infrastructure
  - The Access Tokens although short lived can be used for recon-a-plenty
  - Including, but not limited to: Your entire Entra ID tenant configuration w/o permissions.
- Threat actors are getting more and more creative.