



proofpoint.[®]

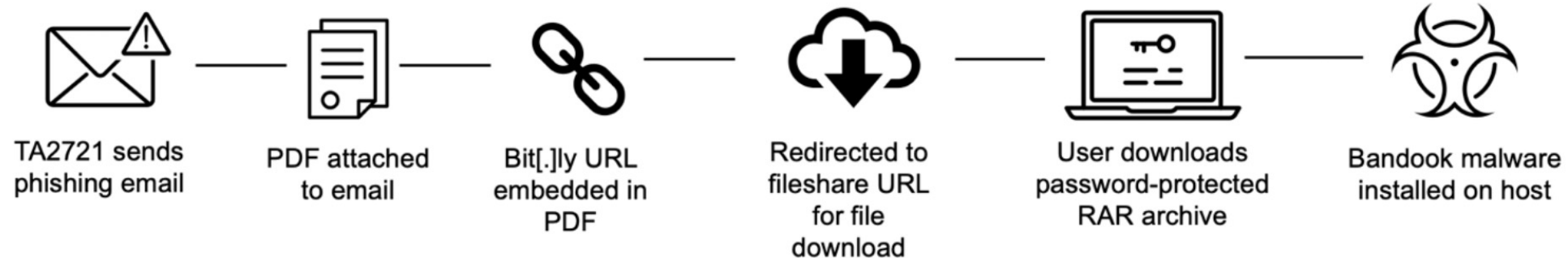
DDX – Detection, Detonation and Config Extraction

Konstantin Klinger, Sr. Security Research Engineer

Lightning Talk @ Botconf 2022, Nantes, 28th April 2022

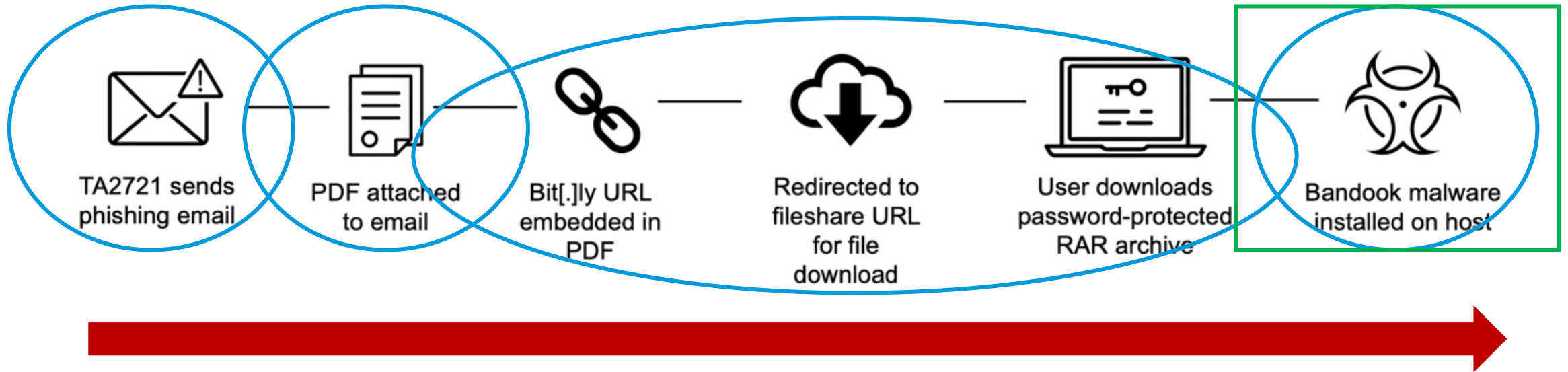
Status Quo / Problem Description

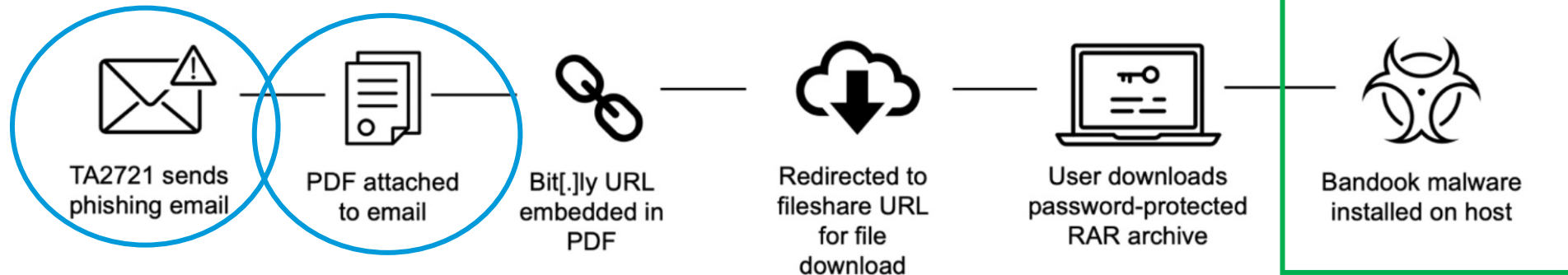
- E-Mail is still number one entry point for actors
 - URLs
 - Attachments
 - Malwareless Scams / Email Fraud
- Complex attack chains with multiple steps until actual malware/payload is dropped are hard to automate, but not impossible




Link to blogpost with all details: <https://www.proofpoint.com/us/blog/threat-insight/new-threat-actor-uses-spanish-language-lures-distribute-seldom-observed-bandoos>

DDX – Detection, Detonation and Config Extraction





COTIZACION REFRITODO INTERNACIONAL, C.A


 cuentasporpagar cpp <cuentasporpagar@refritodo.com>
 To: [redacted]
 Bcc: [redacted]

Reply Reply All Forward ...
 Sun 6/20/2021 10:26 PM


 COTIZACION REFRITODO INTERNACIONAL, C.A.pdf
 35 KB

Buenas tardes, Sres. Refritodo Internacional.
 Reciba un cordial saludo de nuestra parte.
 En los archivos adjuntos encontrará los siguientes documentos:

- COTIZACION y PRESUPUESTO con sello de pagado.

[Gracias por confiar una vez más en nosotros.](#)

Sin más que agregar.
Se despide por

Exhibits behavior characteristic of Bandook (Config Extracted)

Process ID: 3060

C2: r3.panjo.club

C2: http://ladvsa.club/Hayauaia/

C2: http://localhost:9991/KBL/

Port: 7893

AES_CFB_Key: HuZ82K83ad392jVBhr2Au383Pud82AuF

AES_CFB_IV: 0123456789123456

Bonus: Network Signatures (Post Exploitation)

```
NI3B/VGNQ0WJcQAnbGe/G61uhAy4GYmdnmFINKBGqWguDaTfo8UpvbIU+eXf1F0u0FhoF88082Cs j3qSZuK0G4HeBW028K85yCos0WNY0u0RGHxypQL8i0eqyfX7q9ZpaXRjw78bch6bsfFLdfc2t/Q0y6lrxIS5BCNrmv8g==666P4a6i0qGSA==NJK/  
i128QeWJ9IQVT2I=666P4a6i0qGSA==NJK/i128QeWJ9IQVT2I=666P4a6i0qGSA==NJK/i128QeWJ9IQVT2I=666
```

```
!O12HYV~!22535~!192.168.0.107~!XTWGHENV~!dwrsApXT~!Seven~!0d 3h 24m~!0~!5.2~!JN2021~!0~!0~!0~!0~!~!0~!0--  
~!None~!0~!21/6/2021~!
```



- ET OPEN is a **free** ruleset!
- Everything reported by a 3rd party or found in OSINT is in OPEN or will get moved to OPEN once found in OSINT



Questions?

Feel free to reach out to us

/me: @kk_onstantin (kklinger@proofpoint.com)

/threat research: @threatinsight