EMERGING FILELESS MALWARE THREATS

Technical Talk

Presented By: Nimna Sreedharan

DEF CON DC 0471 TRIVANDRUM

About Me

- CyberSecurity Professional for more than nine years
- Proficient at Incident Response and Incident triaging
- Currently part of the Digital Forensics team
- Extremely passionate about Defensive Security
- Part of winning team at Red Team Village-CTF at C0c0n 2019
- Member of DEFCON Trivandrum since past two years

DISCLAIMER

The views, thoughts and opinions expressed in this **presentation** and on the following **slides** are solely those of the presenter, and not necessarily belongs to the presenter's employer, organisation, committee, or any other individual.

CYBER ATTACKS

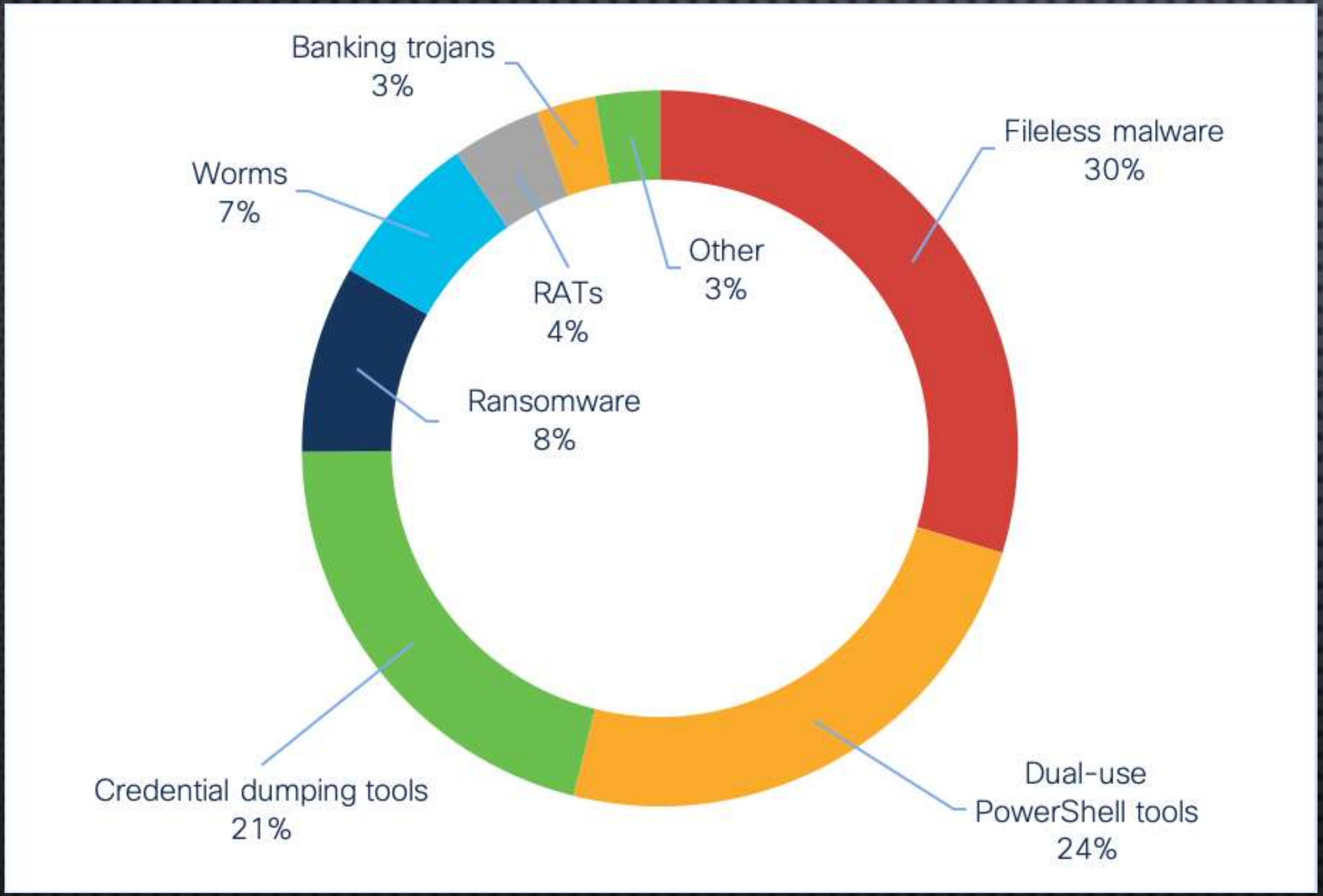
Malware	Zero Day Attack
Phishing	Cross Site Scripting
Man-in-the-Middle attack	Credential Reuse
Denial of Services (DOS)	Password Attack
SQL injections	Drive-by Download Attack

MALWARE?

MALWARE TYPES

- Virus
- Adware
- Rootkit
- Spyware
- Ransomware
- Trojan Horse
- Remote Access Trojan (RAT)
- Key logger
- Fileless

TOP THREE ENDPOINT THREATS



Indicators of Compromise (IoC) breakdown

1. Fileless Malware (30%)
2. Dual-use tools (24%)
3. Credential Dumping tools (21%)

Living off the Land (LotL)

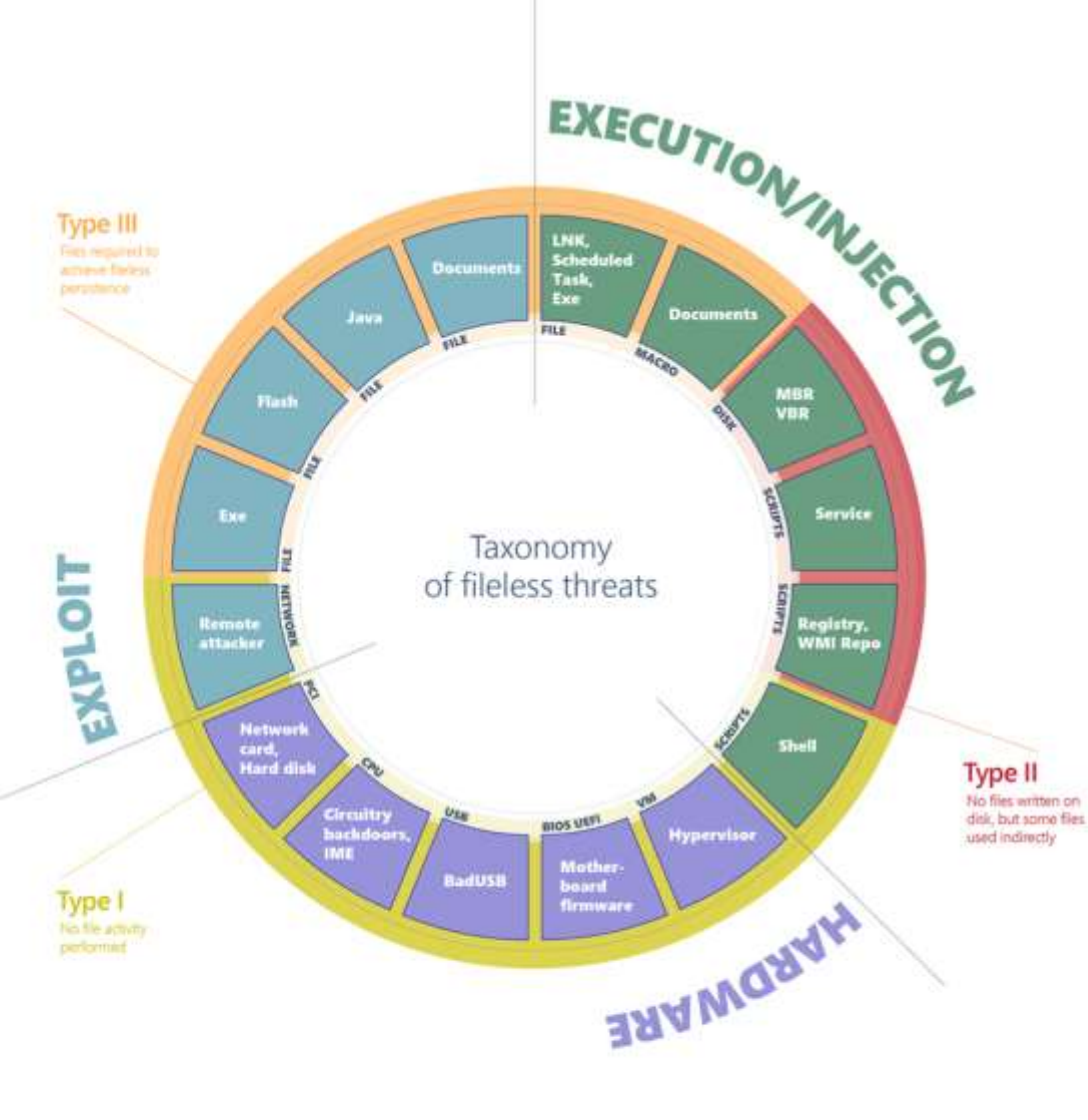
- Can stay undetected for months
- Uses legitimate system shells to download malicious payloads or stage 2 droppers
- Can cause data exfiltration activity
- Most common type of living off the land attack: fileless malware.

What is Fileless Malware?

- No files/executable involved
- 10 times more likely to succeed than file-based attacks
- malicious software that uses legitimate programs to infect a computer.
- abuse tools built-in to the operating system to carry out attacks
- Windows is turned against itself
- Leverages LOTL (Living off the Land)

FILELESS ATTACKS CATEGORIES

- **Type I: No file activity performed**
  - Exploits firmware vulnerabilities
- **Type II: Indirect file activity**
  - doesn't directly write files on the file system, but they can end up using files indirectly.
- **Type III: Files required to operate**
  - have a sort of fileless persistence, but uses files to operate.



DEF CON DC 0471 TRIVANDRUM

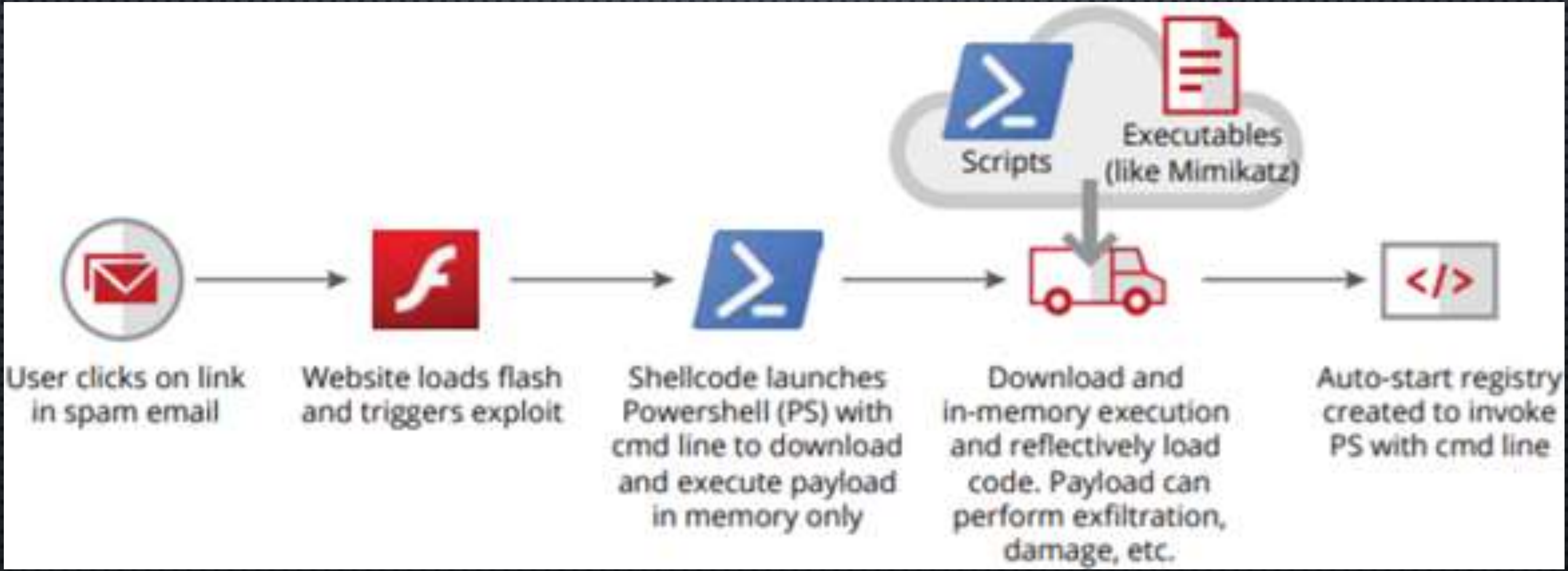
FILELESS ATTACKS: TYPES

- **Registry Resident Malware**
  - installs itself in the Windows Registry
  - Establishes persistence while evading detection
- **Memory-Only Malware**
  - Resides only in memory
  - Backdoor
  - Able to perform reconnaissance, lateral movement, and data exfiltration
- **Fileless Ransomware**
  - Uses exploit to embed code into documents or straight into memory
  - Uses legitimate administrative tools to encrypt hostage files.

LOLBINS LEVERAGED BY FILELESS MALWARE

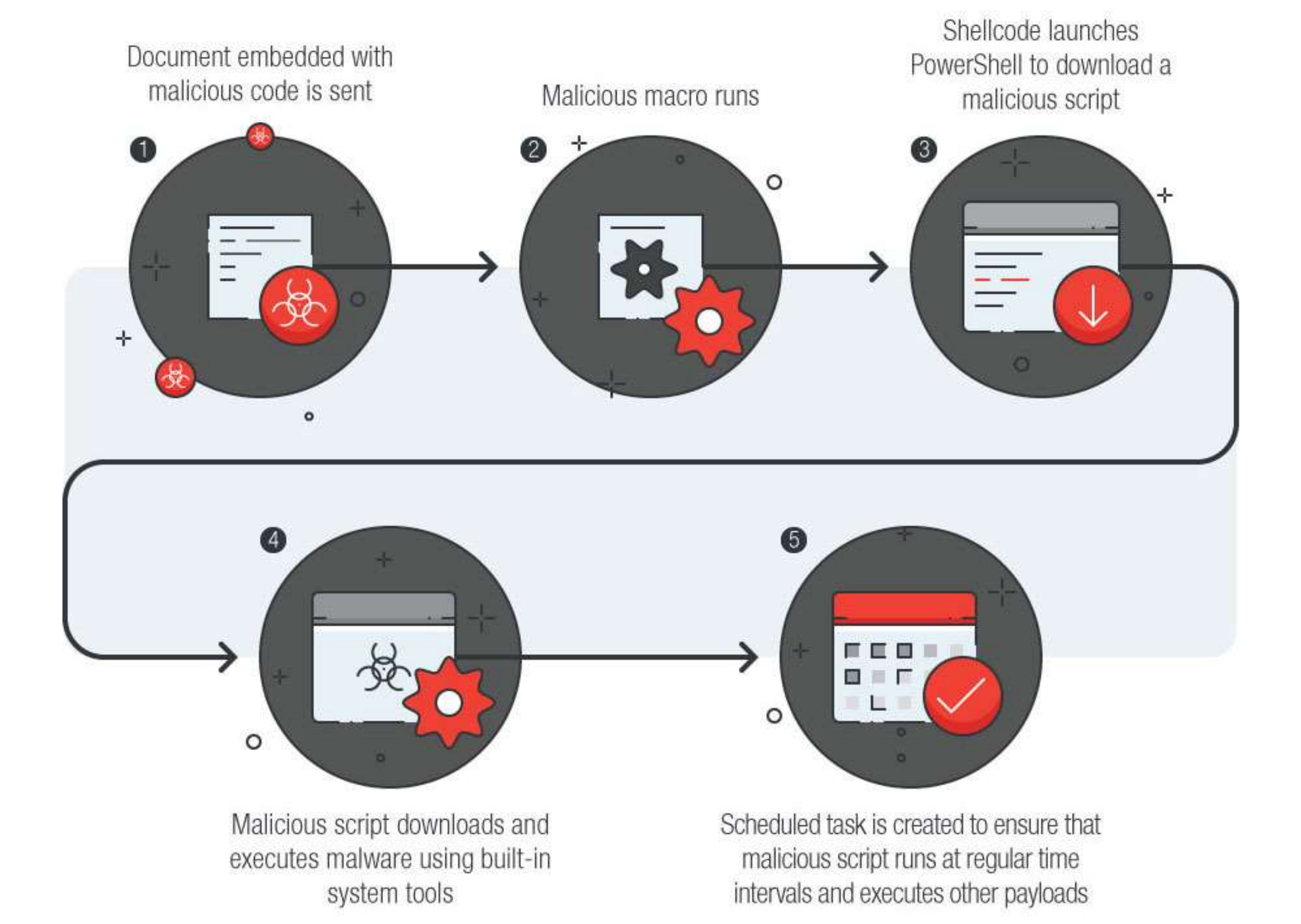
- LotL techniques which use **Windows binaries** to hide malicious activity.
  - POWERSHELL
  - WINDOWS MANAGEMENT INSTRUMENTATION (WMI)
  - .NET FRAMEWORK
  - MACROS

EXAMPLE 1: HOW FILELESS ATTACK WORKS?



Scripts
Executables (like Mimikatz)
User clicks on link in spam email
Website loads flash and triggers exploit
Shellcode launches Powershell (PS) with cmd line to download and execute payload in memory only
Download and in-memory execution and reflectively load code. Payload can perform exfiltration, damage, etc.
Auto-start registry created to invoke PS with cmd line

EXAMPLE 2: HOW FILELESS ATTACK WORKS?



1. Document embedded with malicious code is sent
2. Malicious macro runs
3. Shellcode launches PowerShell to download a malicious script
4. Malicious script downloads and executes malware using built-in system tools
5. Scheduled task is created to ensure that malicious script runs at regular time intervals and executes other payloads

The attackers sent a compromised Word document to their victims through email and enticed users to enable macros in the document. Once enabled, a macro launched a Windows PowerShell script to reach out to specific Internet domains via WMI.

DETECTION: WHY TRADITIONAL AV FAILS

- Attackers depend on tools that are part of the daily workflow of enterprise professionals
- No files. Signature based detection difficult
- LOLBins are a sophisticated threat and detecting them requires advanced tools.
- Windows Registry keys, often overlooked by traditional Av.

How to Combat?

- Ensure Strong Companywide Security Hygiene
  - Patching
  - Raise Security awareness
  - Understand what is normal to identify abnormalities
- Implement Principle of least privilege
- apply behavioural and statistical analysis to identify malicious behaviour rather than the malicious code itself.

DEF CON DC 0471 TRIVANDRUM

WE WOULD LOVE TO HEAR FROM YOU…

- JOIN US TODAY..!!!

- HTTPS://DC0471.ORG/DISCORD
- HTTPS://WWW.FACEBOOK.COM/DC0471/

- IF YOU HAVE FURTHER QUESTIONS , PLEASE CONNECT WITH ME ON DISCORD Q&A CHANNEL @ NIMNA#6201

Thank you