Modelling Duqu 2.0 Malware using Attack Trees with Sequential Conjunction

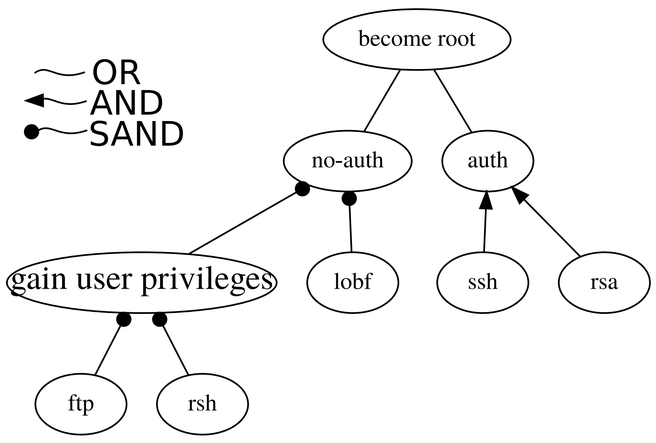
Peter Maynard, Kieran McLaughlin and Sakir Sezer

What is Threat Modelling?

- Allows **visualising threats** and mapping to real world systems.
- Can be applied to networks, software, attacks, and processes.
- Perform analysis of threats which can be used to **identify weaknesses** in systems.
- Can apply **quantification** methods to each path to determine likelihood of a path based on adversary skill, money, possibility etc.

What is SAND?

- Extension for **Attack Trees**.
- Provides Sequential Conjunction operator.
- It has been **formally defined**.



Benefits!

- Perform analysis on major critical infrastructure incidents.
  - Havex,
  - **Ukrainian** power outages,
  - German Steel Mill,
  - Black Energy.
- Identify **common features** between them.
- Features can be used to **detect** similar **sophisticated** attacks.

Initial Compromise and Lateral Movement

Initial Infection

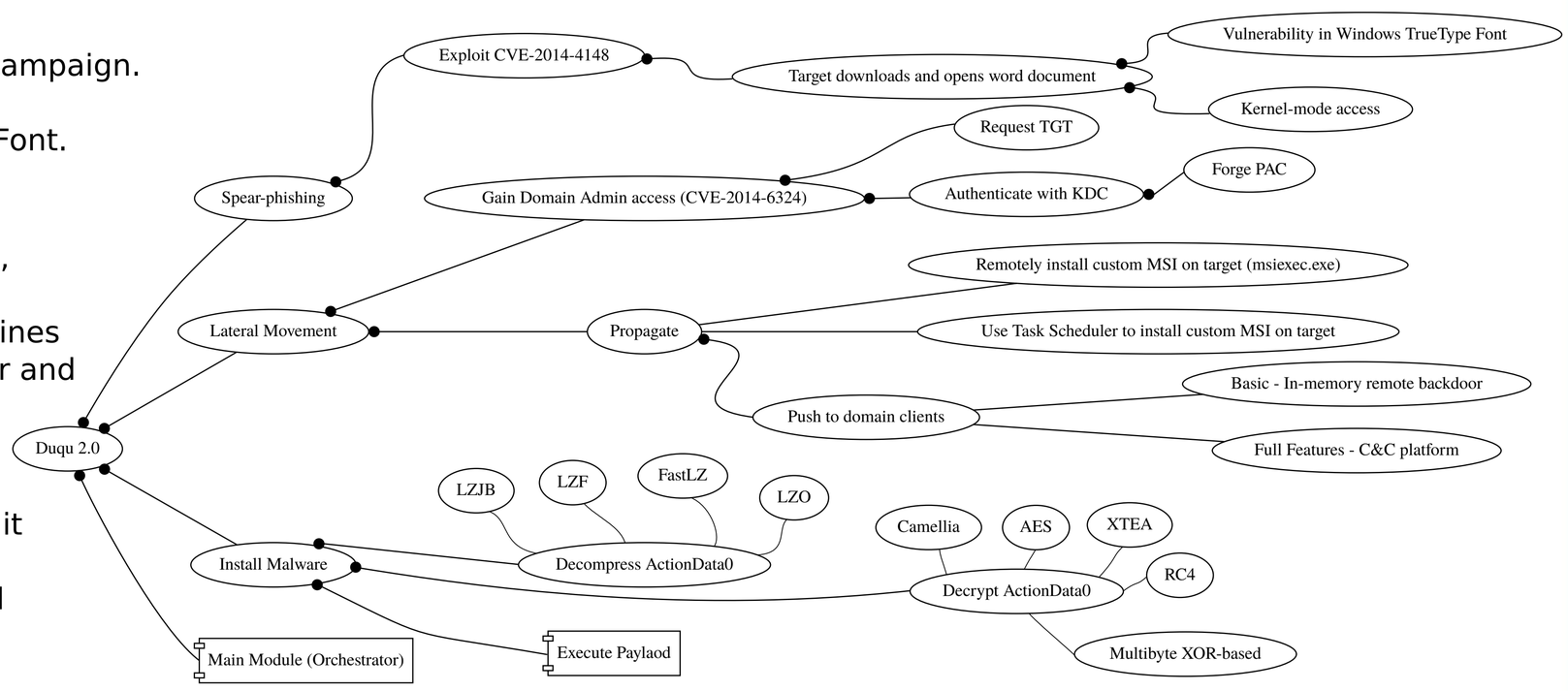
- Duqu was delivered by a targeted spear-phishing campaign.
- Dropper contained in Microsoft Word document.
- Exploits CVE-2014-4148 within Windows TrueType Font.

Lateral Movement

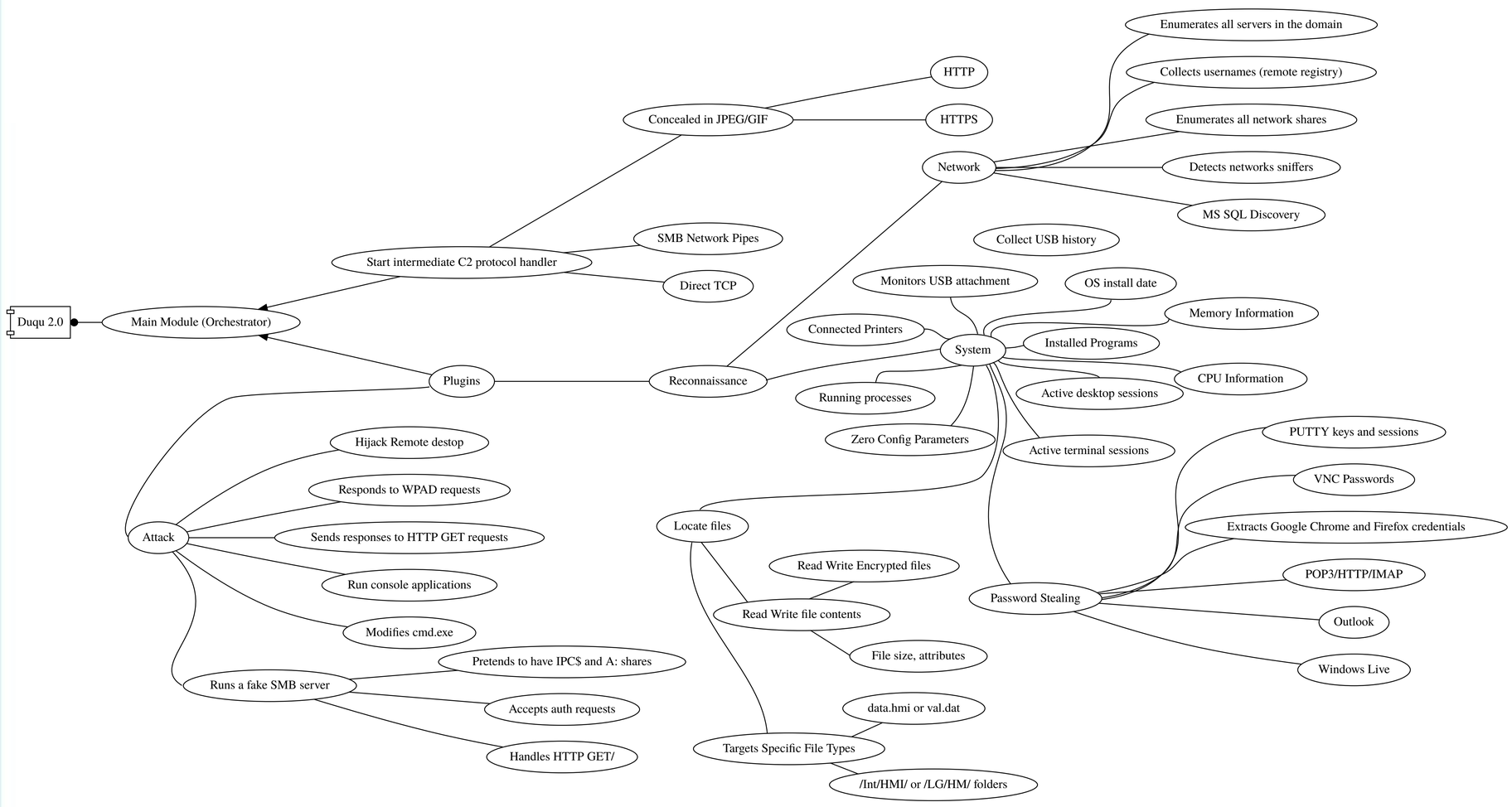
- Gains domain admin access using *CVE-2014-6324*, 'Pass the Hash' exploit.
- Uses its *domain privileges* to remotely infect machines
- *Two variations*. Basic - In-memory remote backdoor and Fully featured remote backdoor.

Installing Process

- To prevent being discovered by anti-virus software it encrypts and compresses itself.
- Uses a varying combination of both encryption and compression algorithms.



Command & Control and Plugin Operations



Main Module Orchestrator

- Starts Intermediate C2 Protocol handler.
- Exfiltrates over SMB and TCP connections.
- Connections bypass detection by concealing data in JPEG/GIF files over HTTP(S).

Plugin Support

- Reconnaissance captures data about the system and the network.
- Records USB, running processes, hardware information.
- Scans the network for Microsot SQL servers, network shares and domain servers
- Able to spoof HTTP requests, Remote desktops, WPAD, and SMB.