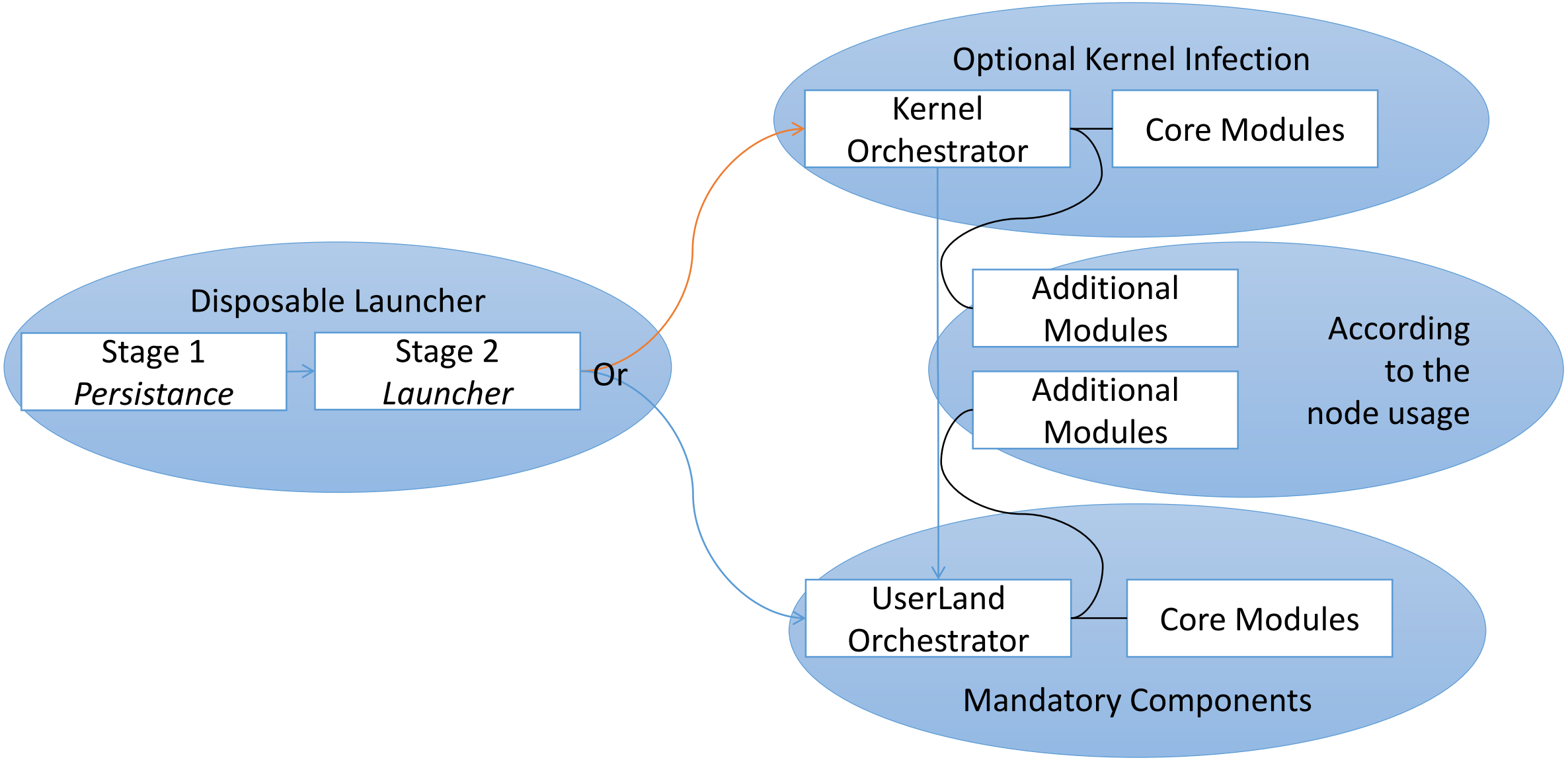
Malware Instrumentation Application to Regin Analysis

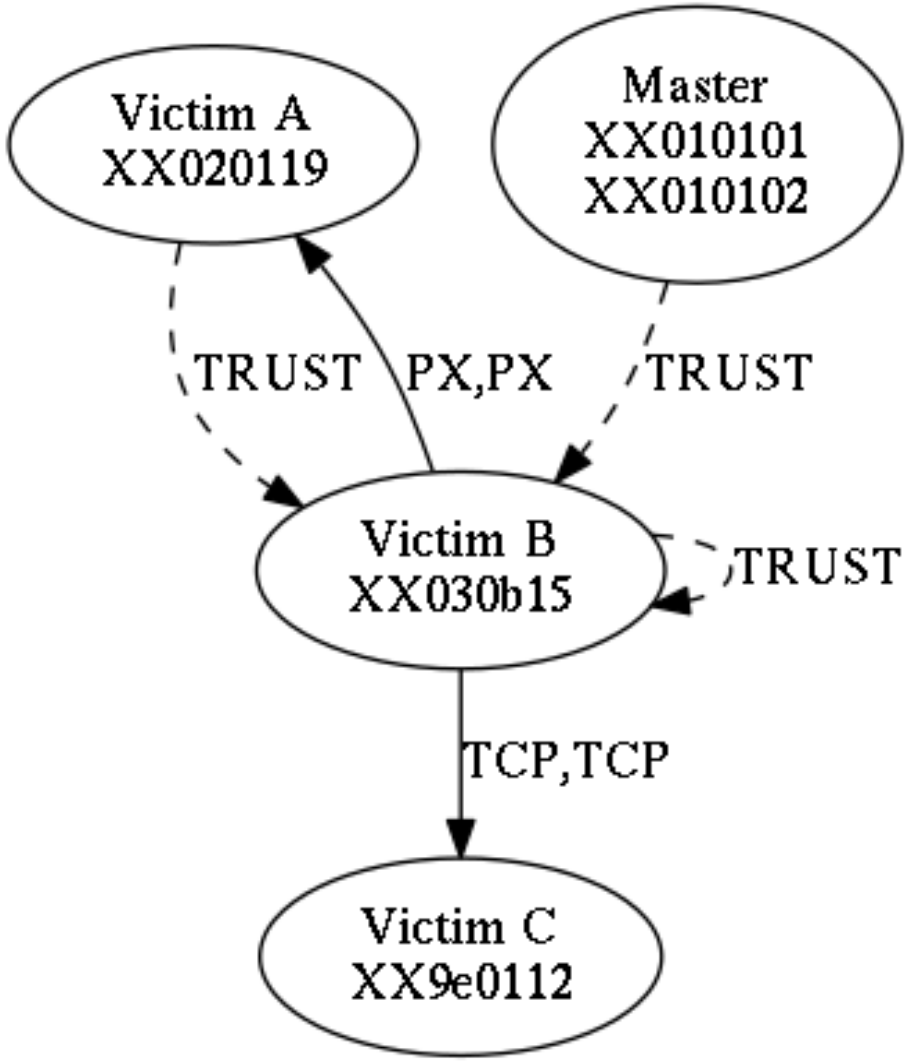
Overview


Optional Kernel Infection
Kernel Orchestrator
Core Modules
Disposable Launcher
Stage 1
Persistance
Stage 2
Launcher
Or
Additional Modules
Additional Modules
According to the node usage
UserLand Orchestrator
Core Modules
Mandatory Components

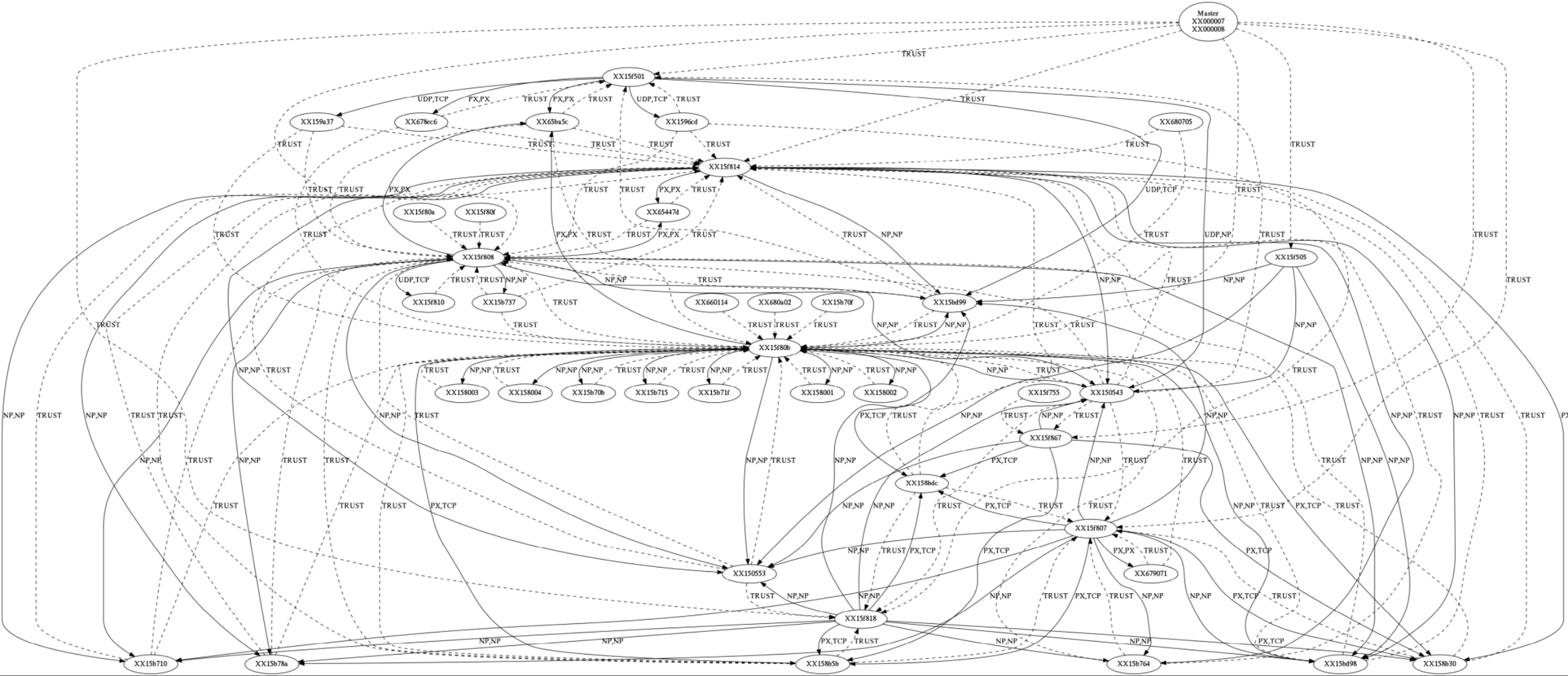
Network Topology: Botnet?

- Connection overlay configuration:
  - List of inbound protocols/port (UDP, TCP, Named pipe…)
  - Inbound is for initialization only, data channel is dynamic
  - List of outgoing connections
- VPN overlay
  - Each node has a virtual IP address
  - Foreign nodes can be reached via routing over the botnet
- Trust overlay
  - Each node has a private key
  - Each node has a list of trusted public keys (trusted peers)
- Masters
  - Master nodes for control over a segment
  - Master report node collect events over a segment

Pivot/Routing



A Typical Infection

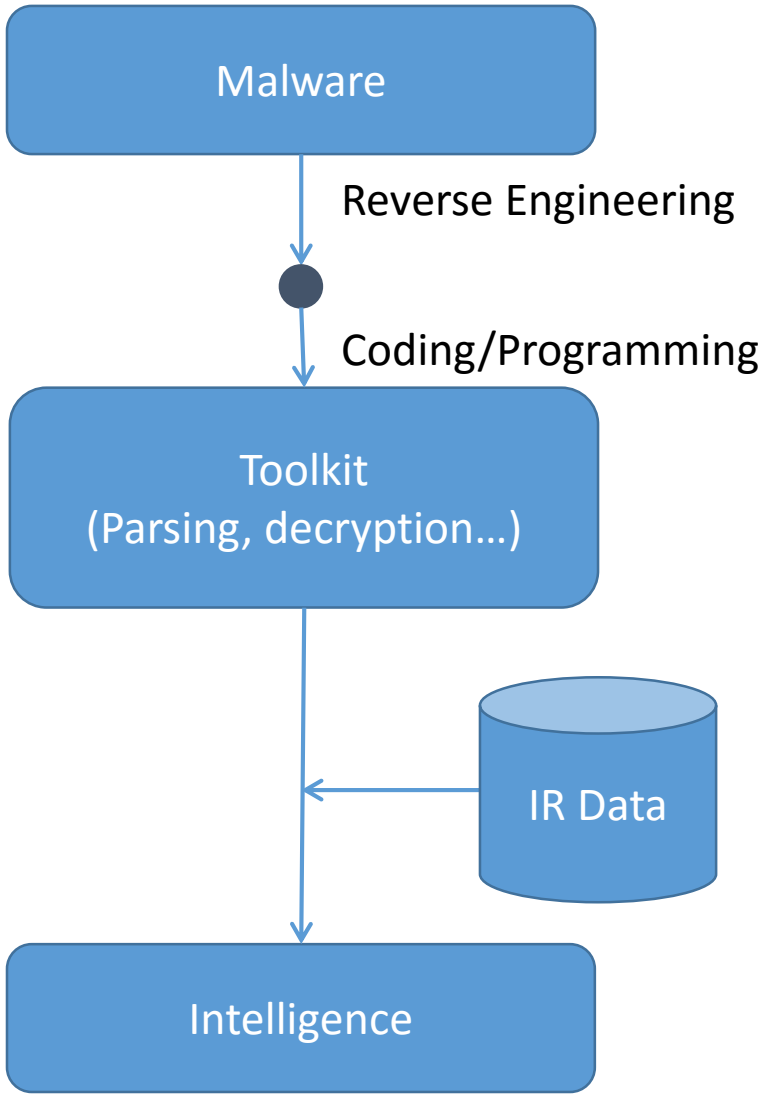


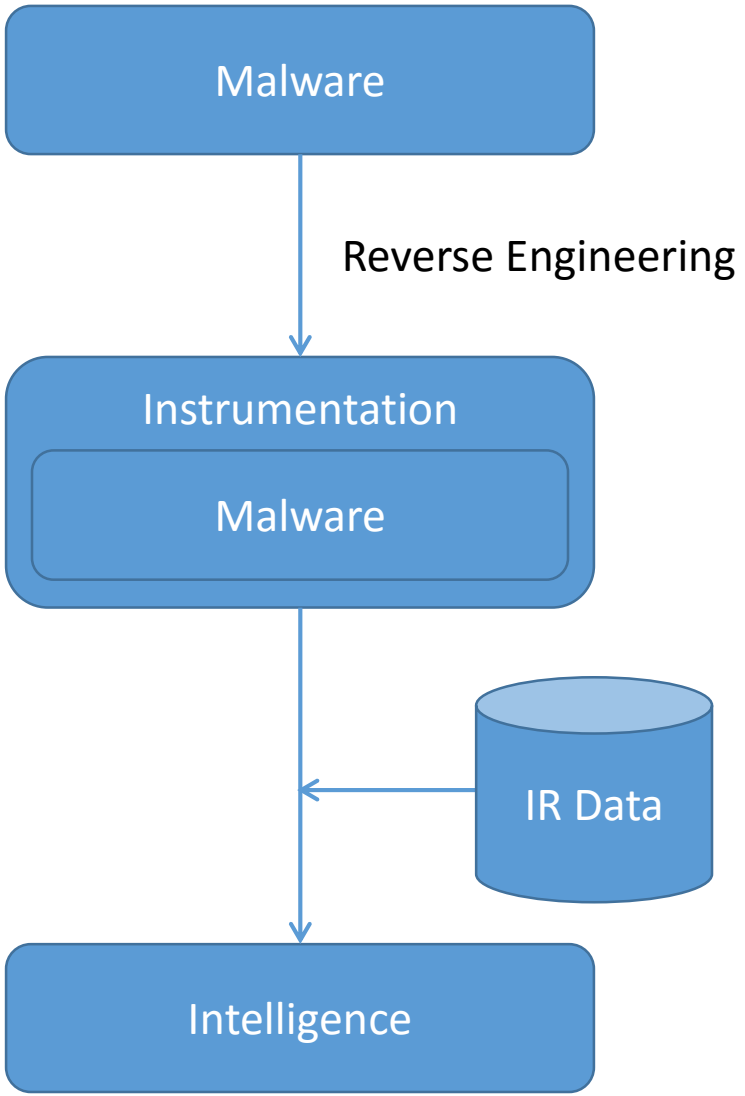
Design

- Service Oriented Architecture
  - Orchestrator
  - Core Modules
    - Cryptography, Compression, Virtual File System, Networking, Logging, TCP, UDP…
  - Additional Modules
    - Intelligence Probes/Sensor/Agents

- RPC: Marshalling, Queueing, Processing

```
mov rcx, [rsp+38h+rpc]
mov r8d, 0Ah                        ;; Module ID
mov rax, [rcx+RPC.module]
mov r9b, 5                          ;; Handler ID
mov rdx, [rax+MODULE.regin]
mov rax, [rdx+REGIN.helper]
mov edx, 7F000002h                  ;; Master node 127.0.0.2
call [rax+HELPER.queueASync]        ;; (void rpc, DWORD node, WORD ModID, BYTE HdlID)
```


Malware
Reverse Engineering
Coding/Programming
Toolkit
(Parsing, decryption…)
IR Data
Intelligence


Malware
Reverse Engineering
Instrumentation
Malware
IR Data
Intelligence

Instrumentation

- Reuse the strong structure and design of Regin
  - Object model
  - Directly query RPC handlers
  - Extract information from live/imaged nodes
- Example: Discover Neighborhood

```
void NETListConns(wchar_t* msg){
    void* stream;
    HELPER->createStream(module0001->instance, &stream);
    NTSTATUS status = HELPER->queueStream(stream, DST_IP, 0x9, 0x5);
    wprintf (L"VIP, ID, *,*,*, ChunkSize, Init mod, Init connstr, Data mod, Data connstr, *,Retry delay, Nb of retry \n");
    reginCodes(stream, status, "IBBBBDWTWTBDBDBBBWB");
    HELPER->freeStream(&stream);
}
tecaRegin> net-conns
VIP, ID, *,*,*, ChunkSize, Init mod, Init connstr, Data mod, Data connstr, *,Retry delay, Nb of retry
0.0.0.2,        01, 96, 28, 00, 00002800, c373, 192.168.226.235:80, c373, 192.168.226.235:443, 00, 00000005, 01, 0000012c, 00, 01, 00, 0000, 00,
```

Defense Perspective

- Usual IOC strategy has limited efficiency: The seek and hide game
  - Disposable loader
  - Encrypted file system
  - Use of legitimate communication channels
  - Botnet structure leveraging 3rd party victims for exfiltration

- Structural detection: Sophistication is a double edged sword
  - Design detection on protocol/structure aspect
  - Backward compatibility will be a challenge for evasion
  - Example: RPC protocol, VFS data structure

- Hunting
  - Use the botnet structure to guide the investigation
  - Climb over sub-segment to obtain a larger view

Attacker Perspective

- Backdoor
  - Access control based on module ID is a bad idea (impersonation attack)
  - Move to hardcoded public key
- Watermark is a low hanging fruit for IDS
- Enhance operations
  - Too many infections and leave behind nodes
  - Clean all artefacts: left-over VFS
  - Avoid cross-victim pivot: a victim might take control over the other

Counter-Intelligence Perspective

- Leverage Regin's own capabilities to observe
  - Logging, RPC traffic capture
- Identify adversary intent
  - Regin is a network of probes
  - Probes feature filters related to the operation objectives
- Use adversary weaknesses

remember me	being larter	delivery failure
ride you	blowjob	delivery notification
asian	breast	delivery status notification
autocad	camel toe	designer
banged	cock	dialost
bed	courtship	discount
bedroom	cum	dreams