Abstract High Level Kill Chain

Reconnaissance
1
- Either public info or other APT
- Potential network scanning
- Potential viewing of running processes and/or installed security services (antivirus, etc.)

Target.Identify

Weaponization
2
- Either preparation of malicious email attachment or url or malicious removable drive

Document.Craft/RemovableDrive.Prepare

Delivery
3
- Email or USB insertion

File.Open

Malware.Spread

Exploitation
4
- Zero day exploit(s) to run, spread, gain privileges without user interaction

Malware.GainsPrivileges

Installation
5
- Makes use of manipulations to keep as little data written to disk, and encryption for obfuscation
- Decryption of own files
- DLL hooking
- Potentially many deletions of files during this process
- Potentially significant discrepancy between installed component and initiating component size

Malware.Install

Command & Control
6
- Test legitimate, common URL that mostly has to do with security or official updates, for internet connection
- Custom encrypted protocols
- HTTP, HTTPS, SSH communications
- Systematic connection patterns SSH, One at a time, etc.
- Sends encrypted, compressed, encoded data
- Receives encrypted, compressed, encoded modules, instructions and updates
- Heavy use of XOR especially and AES

Data.Exfiltrate

Actions on Objectives
7
- Data exfiltration: screenshots, microphone recording, sensitive data, system data, etc.
- Infect nearby machines: local networks, learn about other nearby networks, move laterally through a system
- Sabotage: Cause unsafe, unusual operations to occur
- Eastern Europe, Middle East High Priority Targets

Modules.Send

Malware.Spread

InfectedMachine.Network.Scan