When Governments Hack
Actors, Technology, & Consequences

Alex Rao

October 26, 2020
What is a Nation-State Attack?

• Motives (Politician might be different from normal)
  • Surveillance

• Military options against critical infrastructure

• Financial support from the government – doesn’t need to “make its own money”, as well as administrative/legal

• Not actually government *doing it*, just financing/orchestrating it

• Often legal (if not ethical!) – Eye of the Beholder

• Bangladesh – Bank Heist (still financial motivations!)
Differences from Traditional Attacks

• Motives (Politician might be different from normal)
• Military options against critical infrastructure (unusual/ambitious targets)
• Legality
• Company support (strong arm private companies in cooperative effort)
• Sophistication and Payout (consequences). Even Physical consequences for victims
• Have the resources to throw vast amounts of resources, cyber-gangs just cannot compete (AKA cyber mercenaries)
• APT
• Are different in nature from traditional attacks: Threat Model is quite different
• While powerful, somewhat constrained by political bounds (legality, oversight)
Key Aspects of Nation-State Attacks

Resources
Governments often have far more on tap than private actors

Motives
Motives can be complex and costly; legitimacy and control are often keys

Legitimacy
It’s a government... who’s to say it’s not warranted?
Stuxnet was good from US-Israeli vantage point!

Targets
Often not resource-rich, etc.
Perhaps enough to simply weaken, without return (i.e., “immaterial”)
Case Studies
Bahrain

Small, yet powerful middle-eastern country with a strong, Oil-based economy

Civil Unrest
This was in the middle of the Arab Spring

Constitutional Monarchy
King Hamad has wide powers

Viable but Tense Relationships
Has British RAF and RAV bases, but human rights abuses has caused problems
Motivations

• Very fearful of dissent, or calling into question the legality of government
• Dissent & Insults
• Squashing general activism
FinSpy

• Used Unicode RLO (Right-to-Left Override) to make a filename appear backwards
  • Still works in Windows!

• Wide variety of payloads and capabilities
  • Password recovery
  • Recording of audio and video
  • Hard to detect in the first place

• Sophisticated erasure of traces – memory overwrite

• Full companies (in this case German)
IP Spy

• Discover IP address of victim, for use in identification
• Email with links or images
  • Opening payload pings that IP address, giving an affirmation of ownership
• Others?
IP Spy Anatomy
Consequences

• Identification and Spying on
  • Individual activists
  • Groups
  • Bank Accounts

• Recall – extremely targeted (massive resources for few targets)
Syria

A country that’s seen everything from drought to civil war and third-party extremism. A focal point for most of the world’s powers

All-Out Civil War
Perhaps the most famous civil war of the Arab Spring

Unitary Republic
Semi-Presidential; Western countries refuse to accept results of election

Extremely Polarized Relationships
You either love Assad, or hate him
Motivations

• Ending the war
• Giving Legitimacy
• Tearing down opponent’s legitimacy
• Full blown cyber-warfare
Remote Access Trojans

• Xtreme RAT (XRAT), DarkComet, others
• Also used in cyber crime
• Self-replicating: use host contacts to infect others. Super infectious
• Often spread via ZIPS in private messages
• Capabilities
  • Screen Capture
  • Keylogging
  • Remote shell
Syrian RAT
Consequences

- Hard to exactly identify
- Imprisonment and Policing
- Sexting scandal
- Affects you and exposes surrounding victims
- These attacks are good at lateral movement
- Intimidation, “make an example”
Often cited as the “least repressive” of the repressive regimes, UAE enjoys vast wealth and a tightly-controlled citizenry.

**High Satisfaction**
Among Citizenry, high satisfaction – but most inhabitants are not citizens!

**Constitutional Monarchy**
Not so fast – seven tribal federation

**Good Relationships**
Surprisingly, the UAE enjoys a higher-than-average level of trust with other governments, including the US and Russia.
Motivations

- Surveillance
- Setting up a framework
Remote Control Systems

- RCS, considered “lawful” (ethical...?)
- Far less sophisticated than RAT
- Similar to FinSpy
  - Installs spyware via embedded JAR files
  - 3-Stage Exploit kit installed via variety of methods, including a vulnerable Flash image embedded in a Word Document!
UAE Surveillance
Consequences

• Hard to exactly pin down – mostly defensive
• However, lost property and physical assault seem highly suspicious in timing
High Sophistication

• Attacks often utilize multiple exploits in tandem with each other
• Often, attacks appear to be somewhat hand-crafted and specifically targeted
• Remarkably good understanding of victim vulnerabilities

Traceability

• Attacks often attempted to thwart forensic analysis
• Designed to be difficult to trace back definitively

Consequences

• Imprisonment, curtailing of voices
• Can be Life & Death
• Public Humiliation
Possible Defense?

- Keep your stuff updated
- Use burner phones, pay with cash, generally reduce footprint
  - Maintain anonymity
- Don’t live where this happens (if you can...)
Questions?