The Problem of Protecting High Risk Users

by Eva Galperin and Morgan Marquis-Boire
Whois
Superfriends Go!
Anti-Dissident Campaign

Anti-Dissident Operations Discovered

Skype [Deliver Malware]

Fake Facebook [Deliver Malware]

Fake Youtube [Deliver Malware] [Phishing]

Civil Unrest Begins January 26, 2011

CNN Reporting
Syria’s Torture Centers

“My hands were tied with plastic cuffs behind my back. I was naked sitting on my knees. We were underground. They were beating me with their hands, and batons, and kicks. There were also people next to me being beaten. There was one child who was eight years old who was with us and he was being beaten.”

“They hit the bottoms of my feet with a stick. There was a thick belt tied around my legs so that I couldn’t move them. I was lying with my face on the ground and my feet up. There were two people beating me with a silicon stick. One was standing on my neck. You prefer death. You hope to die. The entire time I was in detention my family knew nothing about me. They didn’t know whether I was dead or alive.”

“They took me underground, blindfolded and handcuffed. Once I stepped into a room somebody kicked me from behind. I fell. They started beating me with everything they could find – sticks, cables, their flats and legs.”

“He beat me with the metal whip on the bottom of my feet and on my thighs, and also above...he pulled me by my toes. I thought that I had reached the end. He pulled my beard with pliers, pulled my nails.... Then they took me and hung me in the shahab position from the door for six or seven hours.”

“There is a wooden beam in the ceiling and they hung me from it with just my toes touching the floor. This was the hardest torture, worse than electricity. I told them I will confess everything – just bring me down. I told them for God’s sake, take me down.”

“There was a chair where the interrogator sat, and a table. Two people in the room were beating me with a one-meter-long cable with metal wire inside and plastic on the outside, accusing me of taking part in the protests and of carrying weapons.”
Hacking Team

Rely on us.
Citizen Journalists Targeted
These seven Moroccan human rights defenders are on trial...

On November 19th, 2015 seven human rights defenders will stand trial in Morocco. Five of them are charged with “threatening the internal security of the State” and face
Ahmed Mansoor and the UAE Five
Spyware Leaves Trail to Beaten Activist Through Microsoft Flaw

by Vernon Silver

October 10, 2012 – 12:28 AM PDT
Threats to Vietnamese bloggers
Vietnamese Malware Gets Very Personal

As encryption has become more prevalent in online communications as a countermeasure against surveillance, attackers have sought to circumvent these measures by covertly installing malware on targeted computers that can log keystrokes, remotely spy on users with their own webcams, record Skype calls, and listen in on the computer's built-in microphone. Sometimes the attacker is a criminal, such as the hacker who used a remote access tool (RAT) to take blackmail photos of Miss Teen USA. Sometimes the attacker is acting in support of a state, like the pro-Assad hackers whose malware campaigns against opposition supporters EFF has been tracking for the last two years. Sometimes the attacker is the government or a law enforcement agency. For example, the NSA’s Tailored Access Operations unit uses covertly-installed malware to spy on targets.

Malware is a tool that most states have their toolbox, and Vietnam is no exception. For the last several years, the communist government of Vietnam has used malware and RATs to spy on journalists, activists, dissidents, and bloggers, while it cracks down on dissent. Vietnam’s Internet spying campaign dates back to at least March 2010, when engineers at Google discovered malware broadly targeting Vietnamese computer users. The infected machines were used to spy on their owners as well as participating in DDoS attacks against dissident websites. The Vietnamese government has cracked down sharply on anti-government bloggers, who
**PACKRAT: KNOWN TARGETING**

**VENEZUELA**
- **TYPE:** Fake organizations
- **TARGETS:** Unknown. Presumed political groups including opposition
- **EXAMPLE:** Fake opposition news website

**ECUADOR**
- **TYPE:** Malware, Phishing, Fake Organizations
- **TARGETS:** Gov. opponents, Journalists, parliamentarians, Gov.
- **EXAMPLE:** Fake opposition site and org. used to spread malware.

**BRAZIL**
- **TYPE:** Malware
- **TARGETS:** Unknown
- **EXAMPLE:** Brazilian lawyers' assn. decoy CV

**ARGENTINA**
- **TYPE:** Malware
- **TARGETS:** Alberto Nisman, other public and opposition figures
- **EXAMPLE:** E-mails with malware sent to high profile political figures.

CITIZEN LAB 2015
South America hacker team targets dissidents, journalists

By FRANK BAJAK Dec. 9, 2015 6:13 PM EST

Ecuadorian journalist Janet Hinostroza poses for a photo at the Teleamazonas tv station in Quito,... Read more
La fuerza del cambio

Política fiscal para la producción

Exoneraciones impositivas para aquellas empresas que agregan y tengan previstos planes de expansión de nuevos componentes tecnológicos, se darán preferencias a sectores productivos que propicien beneficios para la economía. Estrategias de política comercial, la política fiscal de largo plazo que se implemente, se deben centrar en el fomento del crecimiento económico y el desarrollo de la industria.
What is a high risk user?

Activists, Journalists, Human Rights Researchers - Those without security teams.

On a scale of 0 -> Edward Snowden
What do we do?

Outreach - Community Relations / Trust building
What do we do?

Outreach - Community Relations / Trust building

Incident Response - Forensics / malware analysis / Threat intelligence
What do we do?

Outreach - Community Relations / Trust building

Incident Response - Forensics / malware analysis / Threat intelligence

Education - Training / IT Support / Security Helpdesk
What do we do?

Outreach - Community Relations / Trust building

Incident Response - Forensics / malware analysis / Threat intelligence

Education - Training / IT Support / Security Helpdesk

Policy Research - Legal / Law Enforcement
What do we do?

Outreach - Community Relations / Trust building

Incident Response - Forensics / malware analysis / Threat intelligence

Education - Training / IT Support / Security Helpdesk

Policy Research - Legal / Law Enforcement

Advocacy - Awareness / Policy change
What do we do?

Outreach - Community Relations / Trust building

Incident Response - Forensics / malware analysis / Threat intelligence

Education - Training / IT Support / Security Helpdesk

Policy Research - Legal / Law Enforcement

Advocacy - Awareness / Policy change

Follow-up - Other affected parties
What do we do?

Outreach - Community Relations / Trust building

Incident Response - Forensics / malware analysis / Threat intelligence

Education - Training / IT Support / Security Helpdesk

Policy Research - Legal / Law Enforcement

Advocacy - Awareness / Policy change

Follow-up - Other affected parties
Why do we exist?

Large companies don’t / can’t make it a priority to protect this kind of user.

Threat Intelligence companies care about malware not people.
What is being done: increased awareness

State-sponsored warnings

Two-Factor Authentication

Encrypt all the things
An encrypted phish is still a phish
"Most vulnerable" is not a very useful metric. If you aren't targeted, basic protections are sufficient. If you are targeted, none are.
Mis-characterization of threats

People fear what is novel and high profile.

States field multiple teams of differing capabilities.

Targeted attackers may cast their nets broadly, but have realistic expectations of success.
What is to be done?
What is to be done? What industry can do.

Anti-virus industry state-sponsored warnings

Better state-sponsored warnings
What is to be done? What you can do.

When you volunteer, realize that you may not be treated as a unicorn engineer or rockstar programmer.

People may not understand what you do.

It helps if you select something you really care about.
Questions?