CYBER THREATS TO INTERNATIONAL ORGANIZATIONS AND NONPROFITS

INTERNATIONAL ORGANIZATIONS AND NONPROFITS FACE CYBER THREATS FROM THE FOLLOWING ACTORS:

- Advanced Persistent Threat (APT)[1] groups seeking to target international organizations to conduct espionage and give their sponsoring government an advantage in negotiations or agreements. They may also try to take advantage of an organization's trusted relationships to compromise member states.
- APT groups targeting foreign nonprofit organizations operating within their country and focusing on controversial issues. They will probably try to assist the government in monitoring organizations' activities within the country.
- Hacktivists targeting organizations in response to perceived controversy or to otherwise publicize their own views. Hacktivists may launch distributed denial of service attacks intended to knock the victim's websites offline, deface websites, or steal and leak sensitive information to embarrass the victim.

CASE STUDY: APT GROUPS TARGET FOREIGN NGO OPERATING IN CHINA

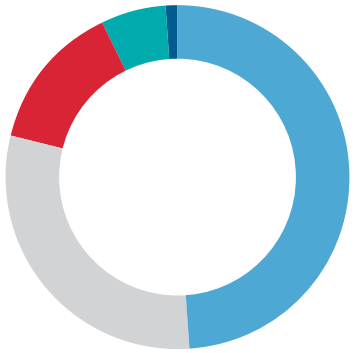
We investigated an intrusion at a non-governmental organization (NGO) with operations in China. Three China-based threat groups had been active in the NGO's network from at least May 2010 until May 2013, although intrusion activity could have potentially begun as early as 2006. They compromised at least 23 user accounts and 86 systems, and stole over 17,000 files, the vast majority of which focused either on the NGO's activities in China, or on its information technology infrastructure and management personnel based at the organization's headquarters. The threat groups stole almost all the files from the NGO's China office, including email repositories for virtually all personnel from 2010 through 2013. Some of the stolen data pertained to specific topics, such as grassroots political campaigns within China.

WE HAVE OBSERVED AT LEAST 9 ADVANCED THREAT GROUPS COMPROMISE ORGANIZATIONS IN THESE SUBSECTORS:

- Grant Foundations
- International Organizations
- Market Polling Research
- Non-Profit Institutions
- Scientific Research & Development Services
- Social Assistance Services

1 Advanced Persistent Threat (APT) actors are assessed to take direction from a nation state to steal information or conduct network attacks, tenaciously pursue their objectives, and are capable of using a range of tools and tactics.

FireEye



TOP 5
MALWARE FAMILIES

- **49%** Gh0stRAT
- **30%** ERACS
- **14%** PHOTO
- **6%** BANGAT
- **1%** POISON IVY

TOP 5
CRIMEWARE FAMILIES

- **39%** RAMNIT
- **25%** PALEVO
- **24%** ZEUS
- **8%** FLASHBACK
- **4%** QAKBOT

CASE STUDY: SUSPECTED CHINA-BASED GROUP HIJACKS NONPROFIT WEBSITE

We investigated an incident at a nonprofit research organization that saw the organization's website hijacked to target the site's visitors. When an Internet user visited the organization's website, their browser was redirected to a malicious website that exploited a zero-day vulnerability in Adobe Flash. If a user's system ran a vulnerable version of Flash, a malicious back-door would be downloaded onto the victim's computer, unbeknownst to the victim. The perpetrators were likely targeting the organization's visitors rather than the organization itself, since we identified no lateral movement or further penetration of the organization's network.

THREAT HORIZON & INDUSTRY OUTLOOK

International organizations and nonprofits will most likely continue to face cyber threats from APT groups in particular, who seek to obtain intelligence with which to inform decision makers. Some factors that may influence future threat activity towards international organizations and nonprofits include their involvement in:

- Operations overseas and in initiatives that the host government views as controversial, sensitive, or a potential threat to either its own legitimacy or domestic stability. Threat actors would likely seek to monitor such an organization's activities.
- Matters of geostrategic or international interest. APT groups from a variety of countries will likely target such organizations and conduct espionage to benefit their sponsoring government.
- Controversial issues or facing their own controversy. Hacktivists may target organizations if there is the perception that the organizations have failed their mission, or are working against a cause that the threat actor holds dear. They may also target organizations if they feel that doing so would assist them in publicizing their own views.

DATA STOLEN FROM INTERNATIONAL ORGANIZATIONS & NONPROFITS

- Event-related Material
- Grant/Scholarship Documents
- Internal Communications & Documents
- Ongoing/Pending Case Documents/ Testimony
- Programs & Initiatives
- Research Reports
- Statements of Work

TOP MALWARE FAMILIES

FireEye most frequently detected threat actors using the following targeted malware families to compromise international organizations and nonprofits:

Gh0stRAT	is a remote access tool (RAT) derived from publicly availablesource code. It can perform screen and audio captures, enable a webcam, list and kill processes, open a command shell, wipe event logs and create, manipulate, delete, launch and transfer files.
ERACS	is a HTTP-based backdoor that generally communicates with IPs over TCP port 80. It can upload and download files, manipulate services and processes, create a reverse shell, act as a keylogger, perform screen capturing, obtain host and username information, etc.
PHOTO	is a DLL backdoor that typically installs itself as a service and can be implemented as a 32-bit or 64-bit DLL. It may extract drivers to employ rootkit functionality by hooking various input output control (IOCTL) devices for the purposes of logging keystrokes and hiding network traffic and registry keys. These drivers may be operating system-specific.
BANGAT	is a backdoor capable of key logging, connecting to a driver, creating a connection to a C2 server, capturing mouse movement, gathering system information, creating and killing processes, harvesting passwords, shutting down and logging off systems, and creating and modifying files.
POISON IVY	is a publicly available RAT that provides comprehensive remote access capabilities on a compromised system. Its variants are configured, built, and controlled using a graphical Poison Ivy management interface available online. It can be configured to produce shellcode, which can be packaged into an executable or combined with an existing executable to hide its presence. It is typically configured to inject multiple shellcode stubs into the explorer.exe process.

TOP CRIMEWARE FAMILIES

FireEye's sinkhole and dynamically shared threat data indicate that the following crimeware variants were the most commonly detected in international organizations and nonprofits:

RAMNIT	is a file-infecting worm that can steal FTP and bank account credentials, remotely execute shell commands, and evade anti-virus software detection.
PALEVO	is an information-stealing worm that spreads over removable drives, network shares, P2P, and instant messenger programs. Infected machines communicate with command and control over UDP port 53.
ZEUS	(aka Zbot) is a family of trojans primarily designed to engage in banking credential theft. It is capable of a wide variety of function, including the ability to remotely execute shell commands.
FLASHBACK	is the most widespread botnet to affect systems running Apple's OSX operation system. It exploits a security flaw in Java in order to install itself.
QAKBOT	is a multi-purpose trojan distributed through browser exploits and dropped by other malicious software. Qakbot is comprised of several components, not all of which are present in every infection. It can spread across network shares and engage in data theft. Typically, stolen data is uploaded to an FTP server where the threat actor can access it.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 / 408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye