The Playpen Cases: Frequently Asked Questions

The Basics

The NIT

Legal Issues

- What should I do if my client is charged, or being investigated for, accessing Playpen or websites like it?

The Basics

What happened in the Playpen investigation?

In December 2014, the FBI received a tip from a foreign law enforcement agency that a Tor Hidden Service site called “Playpen” was hosting child pornography and that its actual IP address was publicly visible and appeared to resolve to a location within the United States. After some additional investigation, the FBI obtained a search warrant and seized the server hosting the site.

Then, in an unprecedented investigation, instead of shutting Playpen down, the FBI continued to operate the child porn website for nearly two weeks. While the FBI was operating the site, it applied for and received a single warrant to send malware to thousands of unsuspecting visitors of the site, exploiting (what we believe was) a vulnerability in Firefox browser code bundled in the Tor Browser to install malware on their computers.

The FBI’s malware—euphemistically called a "Network Investigation Technique" or NIT by the government—searched for and copied certain identifying information from users’ computers and sent that information outside of the Tor network back to the FBI in Alexandria, Virginia. Thousands of computers, located all over the world, were searched in this way.

Once the FBI obtained an IP address from the NIT’s transmissions, it served subpoenas on Internet service providers to learn the names and addresses associated with that IP address. The FBI then obtained warrants to search and seize evidence associated with child pornography at those locations.

As far as EFF is aware, this is the most extensive use of government malware by a U.S. law enforcement agency in a domestic criminal investigation.

How many cases are being charged in connection with the Playpen investigation?

As it stands now, the federal government has prosecuted hundreds of people across the country as a result of this investigation. To date, reports indicate that at least 137 cases have been brought around the country. The government has acknowledged that more than a thousand computers all over the world were infected by its malware.

What is Tor?

Tor is a service that helps you to protect your anonymity while using the Internet. Tor has two parts: software you can download that allows you to use the Internet anonymously, and the volunteer network of computers that makes it possible for that software to work.

When you use the Tor software, the Tor network shields your public IP address by routing web traffic across several different servers or “relays” and encrypting the traffic so it isn’t readily traced back to you. To other computers you connect via Tor, it appears that your connection is coming from the IP address of a Tor exit relay, which can be anywhere in the world.

Additionally, Tor supports a form of anonymous publishing inside of the Tor network itself, known as Tor Hidden Services. A website or other Internet service can make a version available as a hidden service, which is typically accessible only through Tor. Unlike a traditional website, the hidden service site operator and visitors do not observe or learn one another's public IP addresses when communicating this way, so their offline locations and identities can remain hidden from each other.

There are many reasons you might use Tor, including keeping websites from tracking you and your family members, using websites or services which are blocked in your country (for example, getting around the Great Firewall of China), and maintaining anonymity when communicating about socially sensitive information, such as health issues or whistleblowing.

For more about Tor and how it operates:
https://www.torproject.org/about/overview.html.en#thesolution

What is malware?

Malware is an abbreviation for "malicious software"—software specifically designed to gain access to or damage a computer without the owner's consent. Malware includes spyware, keyloggers, viruses, worms, or any type of malicious code that infiltrates a computer. Generally, software is defined as malware based on the intent of the creator rather than on any specific features of the software or code.

What is a "NIT"?

A Network Investigative Technique, or NIT, is a term used exclusively by the U.S. government to refer to the methods or tools it uses to access computers of individuals that have taken steps to obscure or mask certain identifying information, like an IP address.

In the Playpen investigation, for instance, the NIT used by the government is malware that was surreptitiously disseminated through a Tor hidden service. The malware was designed to pierce the anonymity provided by the Tor network by (apparently) exploiting a vulnerability in the Firefox web browser (running as part of the Tor Browser) to place computer code on users' computers that would transmit private information back to a law enforcement server outside of the Tor network

Is a NIT a type of malware?

Yes, undoubtedly. A NIT or Network Investigation Technique is simply a label the government uses to describe the memory-resident malware it used in this and other investigations.

Why does the U.S. government want to use the term NIT instead of malware or hacking?

NIT is a term coined by the FBI. It has no technical meaning. Instead, the FBI chose an acronym meant to minimize the appearance of intrusiveness of its tool. However, rebranding the tools the FBI uses to conduct its hacking does not alter the intrusiveness of or legal consequences that should follow these hacking practices.

THE NIT

How did the malware in the Playpen investigation work?

The FBI has delivered its malware by exploiting a vulnerability in Mozilla's Firefox browser. The initial exploit code downloaded the rest of the NIT malware which then copied certain identifying information from the computer and sent that information back to the FBI without encrypting the data or mathematically authenticating it.

The malware used in the Playpen investigation can be thought of as being composed of at least three critical parts:

1) a generator, running on the hidden service, which created a unique ID for each deployment and transmitted the ID, exploit, and payload;

2) the exploit that took advantage of the vulnerability in the user's software, allowing access to the user's device; and

3) the payload that copied information from a user's device and then sent that information back to the FBI unencrypted and unauthenticated via the Internet.

What is a generator?

The generator is the component of the NIT that generated a unique ID for each deployment and was responsible for delivering that ID, the exploit, and payload to the targeted computer. The unique ID was used to associate a particular user of the site with the information that was ultimately obtained from the payload.

What is a vulnerability?

A vulnerability is a weakness in software or hardware that may allow an attacker to intrude into a user's system.

What is an exploit?

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or some other electronic device. Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service attack.

What is a payload?

In the context of malware, the payload refers to the part of the malware that performs actions chosen by the malware's author or operator, producing effects on or through the affected systems. In this case, the FBI has indicated that the payload of the software that ran on users' computers was designed and used to gather identifying information from those computers and transmit it back to the government.

LEGAL ISSUES

Does the government need a warrant to search my computer using malware?

Yes. The Fourth Amendment protects personal computers from warrantless search and seizure by the federal government.

Did this warrant violate the Fourth Amendment?

Yes, for a number of reasons. The FBI carried out thousands of searches and seizures, in locations around the world, based on a single warrant. The particularity requirement of the Fourth Amendment was designed to prevent precisely this type of sweeping authority.

But I thought the Fourth Amendment doesn't protect IP addresses?

In some cases, courts have found that individuals lack a reasonable expectation of privacy in IP addresses assigned to their devices when those IP addresses *are obtained from a third party*. Here, in contrast, the government obtained the IP address through searches and seizures of *private, personal computers* often located *inside a person's home*. These types of private spaces—homes, an individual's personal computer—represent the core of the Fourth Amendment's protection, and there is no doubt that the Constitution protects an IP address in this context.

Did this warrant violate Rule 41?

Yes. Rule 41 only authorizes federal magistrate judges to issue warrants to conduct searches in the judicial district where the magistrate is located—with limited exceptions that do not apply in this case. The magistrate that issued the warrant here was located in the Eastern District of Virginia. The magistrate thus could not authorize searches of computers located outside of that district.

What should I do if I'm being investigated for accessing Playpen or websites like it?

Find a knowledgeable criminal defense attorney immediately. If you do not think you can afford an attorney, contact the nearest Federal Public Defender in your state. Do NOT communicate with law enforcement until you have retained an attorney.

What should I do if my client is charged, or being investigated for, accessing Playpen or websites like it?

If you are an attorney representing a client in a case related to the Playpen investigation and would like to speak with an EFF attorney about the case, please email info@eff.org.

SECURITY

GOVERNMENT HACKING AND SUBVERSION OF DIGITAL SECURITY

STATE-SPONSORED MALWARE