HOW DO OUTSIDERS TURN YOUR WEBCAM AGAINST YOU?

Ratters, people who use remote access Trojans (RATs) to take control of individual computers and webcams from afar,[1] have a lively marketplace and advice headquarters at message boards like hackforums.net. There, ratters—stereotypically and likely not inaccurately young men—buy and sell "slaves," people whose computers and webcams have been commandeered for the men's vicarious enjoyment. Ratters also trade tips about "slaves" and the best ways to spread RAT software.

While virtually all computers are vulnerable in some way or other to top attackers, ratters, many of whom are novices, often rely on one of a few tricks to convince users to infect themselves. There are some common ways, and luckily, they are often easily avoidable.

FAKE MEDIA

Torrents are a staple of the internet, particularly for those seeking to download media, research, and software. Torrents are small files that help users locate and download content from many users at once using BitTorrent, a protocol designed to enable peer-to-peer sharing and downloading. A report by analytics company Musicmetric, for example, found that in the first six months of 2012 there were 405 million music releases downloaded around the world with the help of torrent files and BitTorrent.[2] Ratters take advantage of the proliferation of torrent search engines by disguising RATs as popular songs and uploading them to the internet for torrent sites.

Ratters search the charts of popular torrented music and upload their RATs named after these songs to torrent sites. Ratters pay attention to ways of gaming the system, including evading torrent sites' internal controls by not uploading too many files soon after registering, using multiple accounts to provide fake positive feedback for a potential download (that is actually infected with software to allow the ratter to turn on your camera), or uploading legitimate files first to boost reputation. Ratters may upload a legitimate version of a song along with a RAT with a name like "PASSWORD TO UNLOCK" or "ESSENTIAL: READ ME FIRST." A user who clicks the disguised RAT .exe may end up with access to the original file but also can be infected at the same time. It's devious, but luckily it's easy to spot. A rule of thumb—if a torrent download requires you to click a link or run a separate file in order to access whatever you were after, it's better to steer clear.

"OMG I CAN'T BELIEVE THAT PIC OF U!!!"

Facebook, Twitter, Chatroom, and Ad Spamming

If you're active on any social networks or chatrooms, chances are you've come across a message and link reading something like, "OMG I can't believe this picture of u!" These spam messages, which, sites like Twitter have fought by limiting the types of links that can be sent via the service's Direct Message function, are one way that ratters recommend spreading their wares. Sometimes, the spam messages will come from people you actually know whose computers have been infected and turned into zombie transmission devices. Alternately, websites and ads designed to look like legitimate products such as the Firefox browser or anti-spyware software may also carry RATs. As librarian and privacy advocate Alison Macrina Tweeted, a Google or Bing search for Firefox actually returned multiple fake Firefox downloads ahead of the actual Firefox website.[3] (No such result appeared in the privacy-friendly DuckDuckGo search engine).

Some lessons are to inspect URLs to make sure they link to the legitimate version of software. You can submit files or links to malware analyzer Anubis[4] or do a web search for the names of unfamiliar programs to check for reports that they are infected. And finally, never click (at least not without responding to the sender for more information) an out of the blue message from a friend on a social network promising a link to a "Crazy Pic" or something like it.

SPEAR PHISHING

While uploading popular songs with associated malware to torrent sites is a common technique to obtain "slaves," there are also tutorials for infecting a specific person, perhaps someone a ratter knows in real life. Without the randomness of posting a torrent and RAT to a website, the creepier process of targeted infection using information from someone's life—"spear phishing"—is more elaborate but also in many ways more dangerous. In both these cases, however, a ratter needs to trick someone in to clicking a link to install the RAT server on their computer.

One example discussed on hackforums.net outlines a hypothetical attack on a college student. In this attack, which the poster's notes can be modified to suit different factual situations, a ratter will reach out to a new student pretending to be a student organization offering free textbooks. The email seems legitimate enough, there may be a flimsy website set up for the fake student group, and the files that eventually get sent are actual textbooks, pirated by the ratter for the purposes of the attack. When there is enough trust between the parties, the fake student organization sends the textbooks along with Readme.txt that tells the student to run a fake "PASSWORD GENERATOR" .exe file, included along with the password protected textbooks. When the victim runs the password generator, they are actually running the RAT, but to prevent any concern, the password generator also provides a legitimate password for the textbook pdfs.

This trade is a bad one for the victim, as their computer and privacy are compromised. Use common sense—it's pretty unlikely that a student organization would randomly email new students and offer free versions of copyright-protected textbooks, no matter how convincing the backstory.

THE MOST DANGEROUS GAME

While each of these methods develops in its own way, a shared aspect is that they rely on tricking someone into clicking a link to run a file that installs and sets up the RAT. Other methods work the same way, with added layers of nuance or difference. One way involves hosting a website featuring a fake video game, where clicking a button in the game will load a fake "error" screen and eventually lead to a download screen for a software update to "fix" the problem. The same website might contain a link to a fake YouTube video advertising the game, where pressing "play" triggers an error designed to trick the user into thinking he or she has to download some update in order to access (actually the RAT). As a rule, reputable websites tend to clearly advertise and contextualize when they are going to offer a download link, so a random download accompanying a click on a video or game should be distrusted.

NOTES

1 Nate Anderson, "Meet the Men Who Spy On Women Through Their Webcams," *Ars Technica*, March 10, 2013, http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/.

2 Enigmax, "Top Bittorrent Countries in the World, Top Torrent Towns in the UK," *Torrent Freak*, September 17, 2012, https://torrentfreak.com/top-bittorrent-countries-in-the-world-top-torrent-towns-in-the-uk-120917/.

3 Alison Macrina, Twitter (Aug. 22, 2014, 11:48 AM), https://twitter.com/flexlibris/status/502890161840328705.

4 Anubis, https://anubis.iseclab.org/ (last modified September 4, 2014).