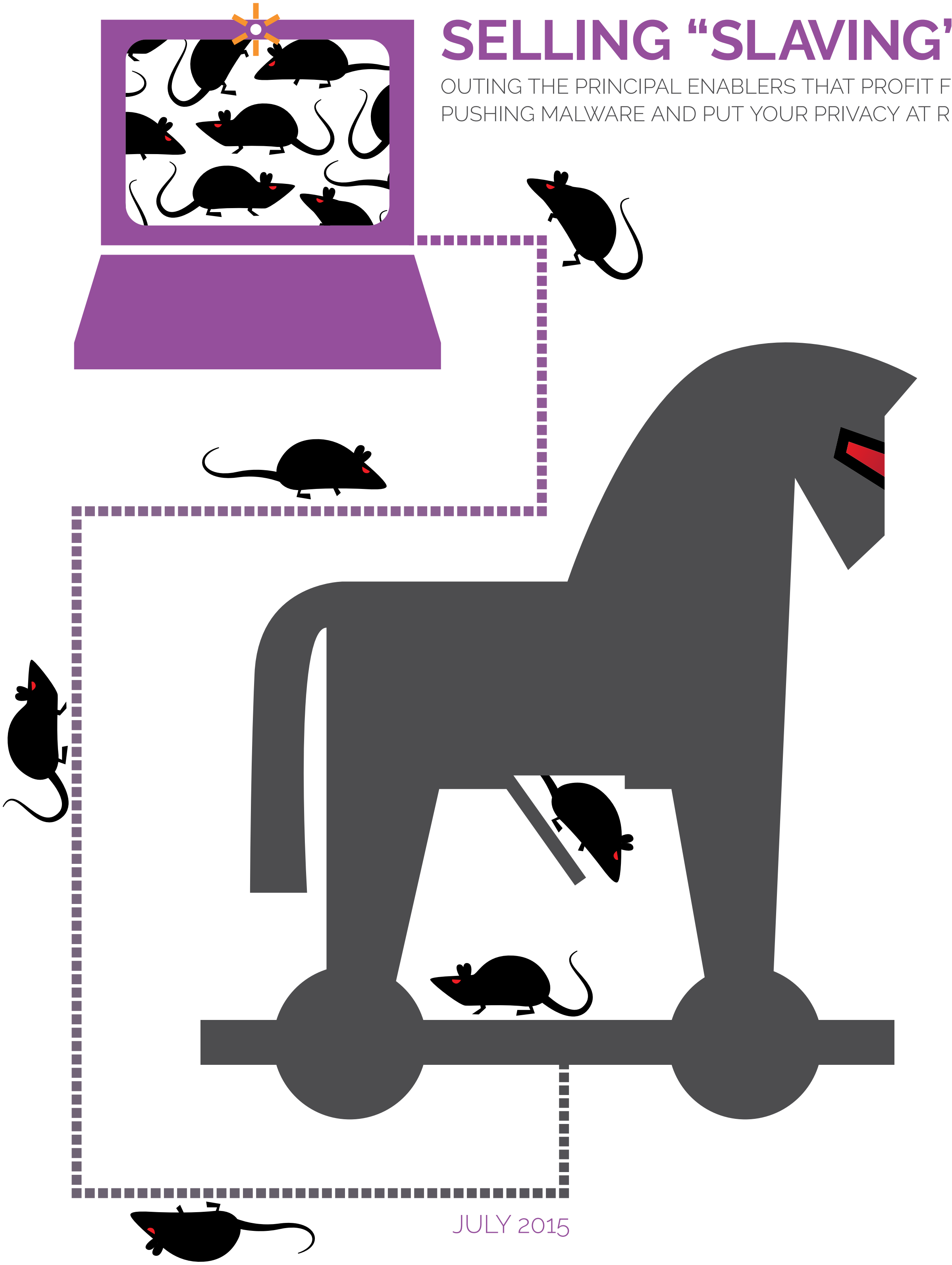


SELLING "SLAVING"

OUTING THE PRINCIPAL ENABLERS THAT PROFIT FROM PUSHING MALWARE AND PUT YOUR PRIVACY AT RISK

JULY 2015

digitalcitizens alliance

TABLE OF CONTENTS

TABLE OF IMAGES

At the time we completed this publication, four of the screenshots listed here are from videos that are no longer up on YouTube. One was taken down around March 2015, a few weeks after Digital Citizens reported the video to a child safety organization. Unfortunately, we've seen that when one is taken down, more are posted just as quickly. Also, we've seen videos with faces of victims exposed up to anywhere from three to five years and getting, in some cases, tens of thousands of views.

For an index of the advertisers Digital Citizens researchers found advertisements for on pages with RAT promotional videos, please go to Appendix A

ABOUT THIS REPORT

The Internet has revolutionized creative thinking and commerce—we are all better off because of the innovators who have developed the breakthrough technology and applications that allow us to share thoughts and images freely.

The vast majority of digital creators want to do good things, but some have used their talents to develop a new generation of malware[a]. Unfortunately making malware, and the disruption it causes, is a growth industry.

That malware is getting into the hands of teens and young adults. With this weapon at their disposal, a growing subset of hackers—or ratters—is disrupting the lives of families across America. We went looking for how they are sharing ideas and tools. We found an increasingly sturdy infrastructure built to cater to aspiring hackers. We saw that these hackers rely on established, trusted companies as well as more nefarious networks to find the resources they need to develop their skills.

The white hats (a.k.a ethical computer hackers) are struggling to develop security applications that keep up with the black hats (someone trying to breach or bypass Internet security[1]). We the consumers are outgunned and outmanned. We don't have the tools needed to protect ourselves. While you are still better off having a 2013 anti-virus program, it won't protect you from zero-day malware anymore than the polio vaccine will protect you from Ebola.

We must realize this perilous moment is not just a product of dangerous hackers and cyber terrorists rushing over the floodgates. We can't ignore the principal enablers of the hackers—a cabal bound together by the desire to draw in viewers with itchy clicking-fingers. To them, tutorials and lessons in malware-making is just another form of click-bait—no different than hit singles or cat videos. Whether they actively assist hackers or simply ignore the products pushed on platforms, these enablers help spread tools exposing businesses and consumers, particularly young women and girls, to great danger.

In our research, we've seen the faces of young people who've been tricked, scammed, and fooled by hackers, or "ratters" who use Remote Access Trojans (RAT) to prey on innocents. It makes it that much more shocking when we see apathy, even resistance, to doing anything to stop the black hats and script kiddies[b] leading this attack on privacy and decency. The hackers and ratters get a boost from a vocal, and well-financed faction within the technology community. This faction, which profits from sharing how to spread malware, stokes the fears of those who believe the Internet's potential as the new land of opportunity could be threatened—simply by demanding accountability for allowing bad actors to thrive. They push back against consumer advocates with screams of "Internet censorship" to shut down any conversation about making the Internet safer, smarter, and more sustainable. The principal enablers of ratters make real people sound almost like "techno-road kill" that were just unfortunate to cross the "data-bahn" as a semi passed through.

[a] Microsoft defines "Malware" as "Short for malicious software. The general name for programs that perform unwanted actions on our PC, such as stealing your personal information. Some malware can steal your banking details, lock your PC until you pay a ransom, or use your PC to send spam. Viruses, worms and trojans are all types of malware." Microsoft, Malware Protection Gallery, Glossary, *available at* http://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx

[b] Urban Dictionary defines script kiddies as "one who relies on premade exploit programs and files ("scripts") to conduct his hacking, and refuses to bother to learn how they work" and "obviously anyone who follows this route aspires to be a blackhat, but most refuse to even dignify them with this term; "blackhat" generally implies having skills of your own." Urban Dictionary, Script Kiddie, *available at* http://www.urbandictionary.com/define.php?term=script+kiddie

To them, there is nothing that trumps "Internet freedom," even if it means opening a door to hackers "slaving" devices of consumers and families around the world. Slaving is the term used to describe the taking control of another user's device.

We feel no business should be making money—not even a penny—from sharing malware used to slave the devices of young women and girls. The malicious materials are only part of the story; this research is about people—the attackers deploying malware, the victims under attack, and the principal enablers making these attacks possible. It is our hope this report will bring increased scrutiny to the ratters infecting our devices, terrorizing our citizens, and crippling companies we know and trust.

Since Black Hat 2014, where we met a college student who told us we should investigate RATs like "DarkComet", "Poison Ivy", and "Cerberus", we have asked one question—how do these malicious files get to so many victims? We see that it is more than just the skill of the malware designer, the pushers of these dangerous applications understand how to maneuver through the digital landscape and find the right platforms on which to leave their traps.

The research coming from cyber security organizations is both devastating and illuminating. We were fortunate to speak with researchers studying malware and learn from their valuable insight. It is our hope to complement the findings of these cyber security experts with stories and images of real people caught in the ratters' traps.

Digital Citizens is preparing a separate report on the history of Remote Access Trojans and more details on each specific kind of RAT. *Selling "Slaving"* looks at the victims, the ratters who push these Trojans, and the enablers connecting the hunters to the hunted.

A WARNING TO CONSUMERS

Digital Citizens researchers used specialized workstations with up-to-date tools and safeguards during its research. We strongly urge that you do not try to replicate this research without adequate protection and expertise. Clicking on links seen on many of these YouTube pages and to anyplace on Hack Forums could put you, your device, and your data in the crosshairs of a ratter.

EXECUTIVE SUMMARY

DIRTY RATS: HOW HACKERS ARE PEEKING INTO YOUR BEDROOM

If you're like most people, your laptop sits on a table in your bedroom, or even on your bed. And from there you may watch a movie on Netflix, talk with a friend on Skype or check your email before you go to bed and maybe even when you wake up.

That computer is a window into your digital world. But what you may not realize is that computer is a window into your private life. The camera on your computer, when hacked, can become a tool to spy on you in your own home. And it's easy.

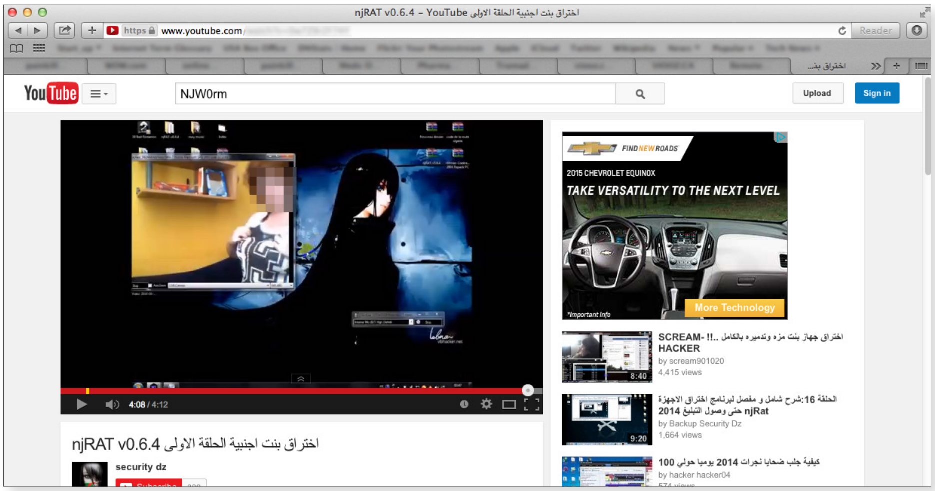
Take the case of 2013 Miss Teen USA Cassidy Wolf, who was the victim of attempted extortion after a hacker took control of her computer's webcam and took private pictures of her in her bedroom. Even though Ms. Wolf bravely stood up to the hacker, who was arrested and sentenced to federal prison, it was a harrowing experience. "I had not one clue of having someone watching me," she told Digital Citizens. "It never passed my mind for the entire year."

How can such a thing happen? The most troubling aspect is how easy it is. It starts with malware on a computer—a virus or program used to gain access to a computer.

Approximately 70 percent of all the malware on the Internet today is some kind of Trojan and the easiest to deploy and use is called a Remote Access Trojan, or RAT.

How do you get malware? Often times by clicking to an unfamiliar website, checking out an online ad on a website, or by downloading a computer program. For example, the Digital Citizens Alliance has found that many content theft sites expose users to malware and other threats. Young Internet users are an easy target because their risk threshold is high and they are more apt to click on unfamiliar websites.

And that is where it gets even more troubling. It's not merely that hackers are peddling malware on unsuspecting Internet users, but they are actively looking to take over the computers, called "slaving," of young girls and boys—and then selling that information online. In effect, they are selling access to our children's bedrooms.



njRAT v0.6.4 – YouTube اختراق بنت اجنبية الحلقة الاولى

https www.youtube.com/

NJW0rm

njRAT v0.6.4 اختراق بنت اجنبية الحلقة الاولى

security dz

SCREAM- !!.. اختراق جهاز بنت مزه وتدميره بالكامل HACKER
by scream901020
4,415 views

الحلقة 16:شرح شامل و مفصل لبرنامج اختراق الاجهزة 2014 حتى وصول التبليغ njRat
by Backup Security Dz
1,664 views

كيفية جلب ضحايا نجرات 2014 يوميا حولي 100
by hacker hacker04

IMAGE 01

• This YouTube video showed a young woman and a young man together in a bedroom. Running next to the video capturing a private moment was a Chevrolet ad.

• At the time of this screenshot, this video had 1,361 views.

A Digital Citizens Alliance investigation found some troubling trends:

→ Using popular search engines to scour the clear web, we found people offering RATs to anyone interested in obtaining the malware. From these results, we confirmed findings from others' previous research that RATs are an inexpensive and technically simple to use tool.

→ Law enforcement confirms that RATs used in 1:1 attacks against consumers are a growing problem. It takes ratters little time to slave hundreds of devices. From there, they can gather private information off those devices, which they can then use to "sextort" the owners of the devices. The ratters frequently take control of devices in girls' bedrooms, take pictures of the girls when they are unaware of the hack, then threaten to release the pictures to wider audiences unless they comply with a ratter's demands. It is difficult to know how many people's computers have been "slaved" as a result of a Remote Access Trojan attack, because victims are often scared and ashamed to come forward.

→ Using the popular hacker chat page Hack Forums, we found ratters selling slaved devices and thereby making money from their malicious attacks on consumers. Girls' devices sold for more than boys.

→ Also on Hack Forums, ratters shared tips about best practices. We captured multiple chats with ratters saying that YouTube and "content theft" sites (i.e., The Pirate Bay, Kickass Torrents, and other sites that provide unlicensed movies and music) were the best places to "spread" RATs.

→ In almost eight months of searches on YouTube, we found thousands of RAT tutorials. The tutorials included many that showed how to use and spread RATs; links where ratters could download the malware; and examples of RATs successfully deployed showing victims' faces and IP addresses. We found IP addresses potentially connected to devices in 33 states and dozens of other countries.

→ Roughly 38 percent of the tutorials for the best-known RATs had advertisements running alongside the videos. The advertising we found included well-known car companies, cosmetics, and even tickets to New York Yankees' baseball games. YouTube's parent company, Google, is positioned to get revenue from the sharing of these malicious tutorials that target innocents. By allowing advertising to remain next to these tutorials, YouTube also provides another stream of revenue for ratters. Using the partner program, ratters are poised to get a cut of advertising revenue from Google.

→ Also on Hack Forums, we found experienced ratters recommending content theft sites to script kiddies looking for tips on how to spread RATs. We found YouTube tutorials demonstrating how ratters can use known content theft sites like Pirate Bay and t411 to build deceptive materials like malicious links and PDFs. These materials are left on content theft sites like traps left to catch animals.

This is a growing problem that threatens to shatter the sense of security that we should have when in our homes. And it preys on the most vulnerable—young people who may feel ashamed or afraid to tell their parents about the threats.

So what can be done about it? From our investigation, Digital Citizens recommends:

→ The creation of awareness programs to alert parents and young people to the potential threat they can be exposed to when clicking on unfamiliar websites and ads or downloading sketchy programs.

→ That parents talk with their teen and pre-teen children about computer safety and let them know to come to them if any online behavior makes them uncomfortable or nervous. Digital Citizens investigation found that teens are apprehensive about letting their parents know their computers are compromised.

→ That law enforcement gets additional resources to increase regulation and awareness of computer-related crimes. One of the best deterrents is seeing hackers punished for illegally invading the privacy of their victims.

→ A solution exists, but it will require Google to change the way it approaches this issue. When Google is serious about solving a problem, it assigns a human team to do what an algorithm clearly can't. Bringing in human teams helped block tens of thousands of search queries for child pornography and to ensure the quality of apps on Google Play. Hacking victims deserve the same concern and protection. Google should assign a human team to reviewing these videos and immediately cease advertising on such video platforms. These victims should not be clickbait and ad revenues from slaving tutorial videos can't be worth the pain and suffering they cause.

One thing is clear: this is a serious issue that cannot be swept under the rug. That is what the hackers are counting on so that they don't get caught and punished. And given the increasing sophistication of technology and therefore criminal opportunity, this problem is likely to get more complex.

To stop the hackers will take a concerted effort of parents, young Internet users, safety groups and law enforcement. If we confront this issue head on, we can ensure that our window to our digital world is not an unwelcome entry point to invade our personal privacy.

WHAT CAN RATTERS DO?

The term "slaving" a computer is no exaggeration. Perhaps the simplest and most popular slaving tool is a RAT. One of the six kinds of Trojans, RATs are malicious code that can be disguised as documents, photographs, videos, and songs to trick targets into downloading the malware onto a device.

Whether it is using the device's functions or sifting through files the user has stored—whatever you can do, the ratter can do. Gary S. Miliefsky was a founding member of the Department of Homeland Security and is now Chief Executive Officer of the mobile app security firm SnoopWall. In his report *2015: Year of the Rat—Threat Report*, Miliefsky explains that ratters can:

→ Download, upload, and delete your files (potentially even clearing a hard drive completely);
→ Steal passwords, credit card numbers, emails, and files;
→ Watch you type and log your keystrokes;
→ Watch your webcam and save videos;
→ Listen in on your microphone and save audio files; and
→ Use your computer for a distributed denial of service ("DDoS") attack.

This last item is important. A ratter seldom stops with one slaved device. Your device is just one step in a ratters' effort to "spread" RATs and other malware. If someone has your personal computer, then your phone, tablet, and work devices are not far behind. The jump to your company's computer could lead the ratter to the corporate network and your office's resources.

Once in command of your devices, your email address book, private emails, credit cards, and password could be next to fall. As Miliefsky said: "If you get infected with one of these Zero-day RATS, you're not only a victim, you are an accidental accomplice."[2]

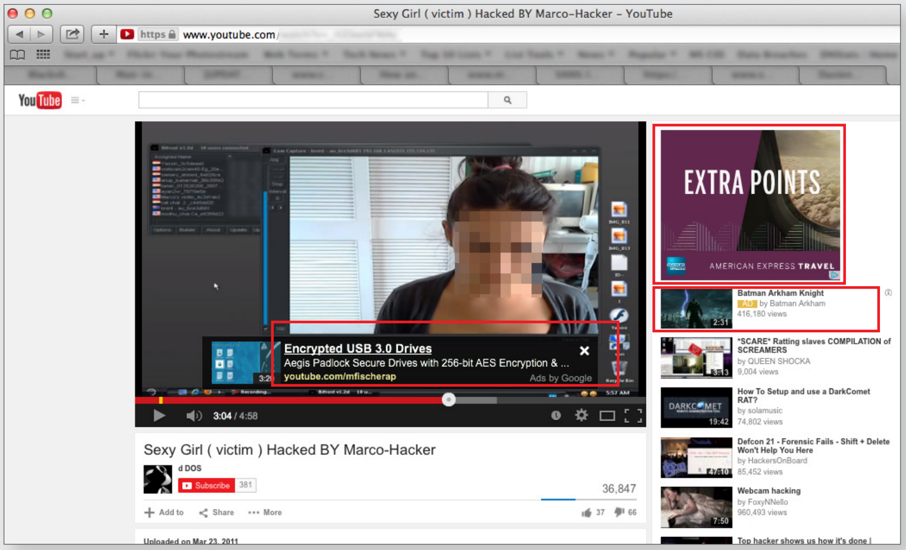
Making it simple—RATs are an easy to use, inexpensive tool frequently used to spy on women, and then exploit them for money and/or sexual favors. They are also a weapon of war used by enemies of democracy to target and attack their adversaries. RATs are frequently used in corporate espionage missions, allowing hackers to pull off many of the embarrassing and debilitating strikes against U.S. corporations.

THE RAT WORLD

Remote Access Trojans studied in this project include:

» Adwind
» AndroRAT
» Back Orifice
» Bifrost
» Blackshades
» Black Worm
» Bozok
» Carbanak
» Cerberus
» CyberRAT
» Cybergate
» DarkComet
» Dark DDoSeR
» Dyre / Dyreza
» Explosive
» Havex
» Kraken
» NanoCore
» Njw0rm
» njRAT
» Pandora RAT
» Poison Ivy
» Predator Pain
» ProSpy
» Regin
» ShadowTech
» Snake RAT
» Sir DoOom
» Sub7
» Trojan.Laziok
» Xtreme RAT

SELLING "SLAVING"



Sexy Girl (victim) Hacked BY Marco-Hacker – YouTube

https www.youtube.com/

Encrypted USB 3.0 Drives
Aegis Padlock Secure Drives with 256-bit AES Encryption & ...
youtube.com/mfischerap
Ads by Google

Sexy Girl (victim) Hacked BY Marco-Hacker
d DOS
Subscribe 381
36,847
Uploaded on Mar 23, 2011

Batman Arkham Knight
AD by Batman Arkham
416,180 views

SCARE Ratting slaves COMPILATION of SCREAMERS
by QUEEN SHOCKA
9,004 views

How To Setup and use a DarkComet RAT?
by solamusic
74,802 views

Defcon 21 - Forensic Fails - Shift + Delete Won't Help You Here
by HackersOnBoard
85,452 views

Webcam hacking
by FoxyNNello
960,493 views

Top hacker shows us how it's done |

IMAGE 02

• By controlling a webcam, someone broke into the bedroom of this girl and then shared the video with the world.

We have blurred the picture of the girl, who we believe was just a teenager when this video was made, to protect her identity. Unfortunately, virtual peeping toms have violated her privacy almost 37,000 times. So many visitors have come to peek at her that YouTube is selling ads to pitch everything from cars to computers to sundries to those coming to visit.

This particular video includes three ads—inside the red boxes and circle. Much of the ad revenue from this post can be split between YouTube and the hackers who posted the video. The picture is only part of the story, as you will see on page 17 where we include part of what these ratters said about their victim.

There are all kinds of victims who have had their devices slaved—corporations, political leaders, and even average families. But corporations and governments have the resources to pay for the finest security (and often, even that isn't enough to stop a hacker). What about those of us armed with only a firewall[c] and anti-virus program? Families don't have the most up-to-date security designed to stop the criminal who doesn't need to break a window or pick a door lock to steal your financial information, family photos, as well as your contacts and password lists. He only needs a keyboard and the newest Trojan.

RATs can be a valuable piece in a skilled hacker's toolkit. They may be a tool for a mission of corporate espionage and economic disruption, or a stand-alone weapon used in a 1:1 attack by a "script kiddie" on a high school classmate.

[c] TechTarget defines a firewall as "a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules." http://searchsecurity.techtarget.com/definition/firewall

IN ORDER TO HIGHLIGHT PORTIONS OF THIS AND OTHER SCREENSHOTS FROM YOUTUBE AND HACK FORUMS, DIGITAL CITIZENS ALLIANCE HAS OUTLINED IN RED AND/OR MAGNIFIED CERTAIN ELEMENTS.

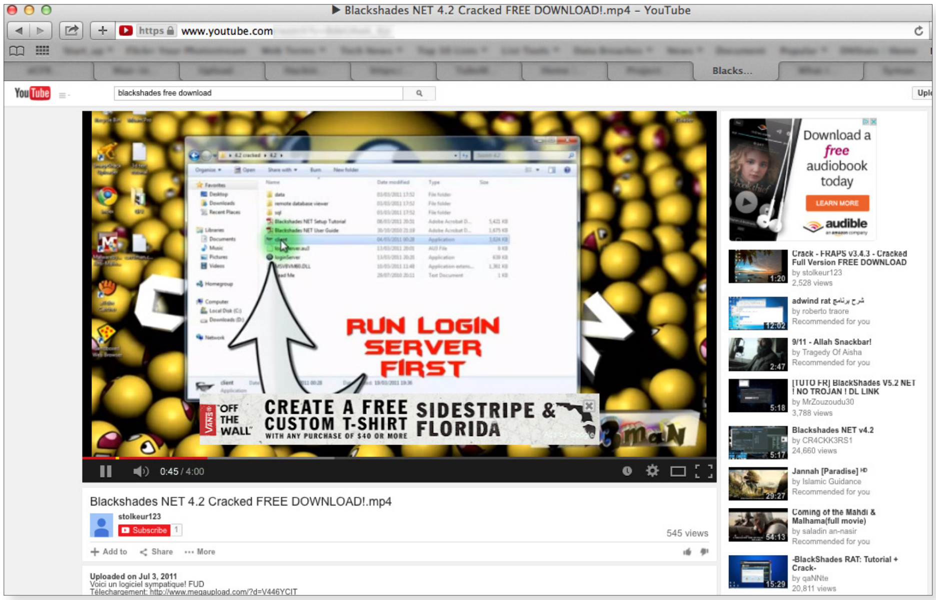
CHEAP, EASY-TO-USE MALWARE THAT PAYS FOR ITSELF

This dangerous, malicious software is easy to find, acquire, and use. Security expert Brian Krebs wrote in his popular blog, Krebs on Security, that one of the most popular RATs, Blackshades, "was a tool created and marketed principally for buyers who wouldn't know how to hack their way out of a paper bag."[3]

"Whether it's the family computer or the office network, most have the same vulnerability, and when people say this is a very sophisticated attack, it's really not," said Miliefsky, who then made a critical point that we also found in our research: "It's about patience." Remember that point when we tell the story of Cassidy Wolf.

As you see in the screenshot (image 3) from YouTube, you can find free RAT downloads marketed there. If it is free, it is likely an older version of the malware. Updated or modified versions of many RATs can be found for between $10 and $50. It wasn't always that easy. In 2013, RATs like DarkComet and Blackshades cost between $50 and $250. Then, according to researchers from Dell SecureWorks[4], leaks making the source code available to the general public sent prices plummeting.

And cyber security analysts have seen the marketplace for RATs take root. Bob Rudis, co-author of Verizon's *2015 Data Breach Investigations Report*, says "there is an entire economic segment basically for cybercriminals where they have both the ability to order these tools, in a very Amazon-like fashion—it's actually a pretty slick portal in some cases, and not only order the tool, but get help customizing the tool. There is a very low barrier to entry for utilizing these things."


▶ Blackshades NET 4.2 Cracked FREE DOWNLOAD!.mp4 – YouTube
https www.youtube.com
Blacks...
YouTube
blackshades free download
Upl
RUN LOGIN
SERVER
FIRST
"OFF THE WALL"
CREATE A FREE CUSTOM T-SHIRT
WITH ANY PURCHASE OF $40 OR MORE
SIDESTRIPE & FLORIDA
0:45 / 4:00
Download a free audiobook today
LEARN MORE
audible
Subscribe
Add to
Share
More

Blackshades NET 4.2 Cracked FREE DOWNLOAD!.mp4

stolkeur123

545 views

Uploaded on Jul 3, 2011
Voici un logiciel sympatique! FUD
Télechargement: http://www.megaupload.com/?d=V446YCIT

Crack - FRAPS v3.4.3 - Cracked Full Version FREE DOWNLOAD
by stolkeur123
2,528 views

adwind rat شرح برنامج
by roberto traore
Recommended for you

9/11 - Allah Snackbar!
by Tragedy Of Aisha
Recommended for you

[TUTO FR] BlackShades V5.2 NET ! NO TROJAN ! DL LINK
by MrZouzoudu30
3,788 views

Blackshades NET v4.2
by CR4CKK3RS1
24,660 views

Jannah [Paradise] HD
by Islamic Guidance
Recommended for you

Coming of the Mahdi & Malhama(full movie)
by saladin an-nasir
Recommended for you

-BlackShades RAT: Tutorial + Crack-
by qaNNte
20,811 views

IMAGE 03

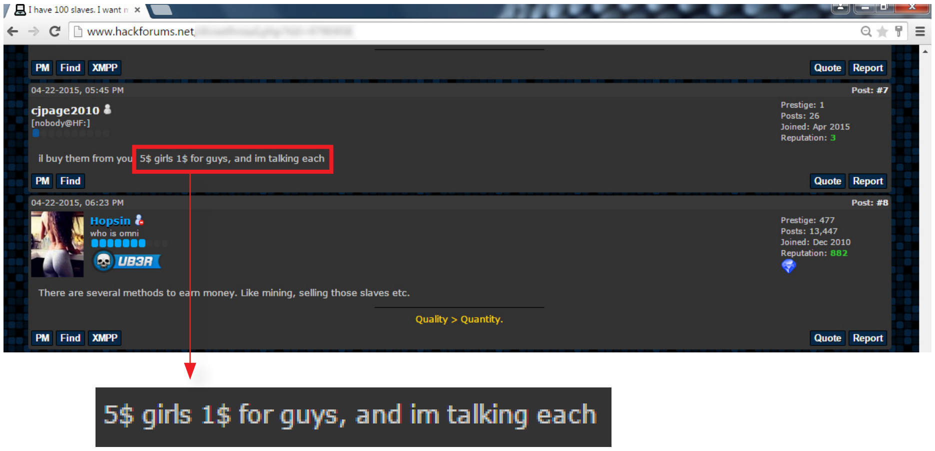
• Below the video, viewers could click on a link where they could "tèlechargement" (French for download) the video.

So while the cost to get started is low, the opportunity to make money quickly as a ratter is great. Digital Citizens researchers visited the popular hacker chat site Hack Forums to find "the voice of the hacker." There are more than 1.5 million posts that discuss acquiring, creating, and spreading RATs (as of 7/22/15). Image 4 shows one example of a Hack Forums participant offering access to the devices of girls for $5 and guys for $1.

Consider that on day one, a ratter can get dozens of victims in a single sitting. If they struggle with the program, there are plenty of other ratters willing to help—either by sharing advice in tutorials found on YouTube or direct contact via chat rooms like Hack Forums, which functions as something like a customer service department for would-be ratters. Laura Eimiller, Press Officer for the FBI's Los Angeles Field Office, said "individuals interested in targeting victims can find what they need and learn how to implement a program online without leaving their bedroom."

James Pastore was the lead prosecutor in Operation Dirty R.A.T.—the multi-national law enforcement sting that brought down the cabal behind Blackshades. He got a first hand look at the pushers of malware and the ratters they helped spawn. Now an attorney in private practice, Pastore told Digital Citizens: "There's a kind of meanness about it, but also a little bit of a distance because they are behind a keyboard. They maybe don't . . . comprehend, or aren't mature enough to comprehend, the real harm that they're imposing on people. And it's a shame because there are real people that are being victimized. It becomes a bit game-ified and I think that is in large part due to the population that—in my experience—is using these types of RATs."

Victims often struggle with damage done from these attacks. Georgia Weidman is an ethical hacker. As the Founder and Owner of Bulb Security and the mobile security testing startup, Shevirah, Weidman has been called in to help control breaches, discover what was stolen, and, if possible, determine the source of attacks. She has helped businesses and individuals after attacks using RATs. She said: "There's a lot of shame in it, particularly when it involves compromising videos or images. I think it is important for victims to know how prevalent it is, how even security researchers fall victim to these sorts of attacks. You haven't done anything stupid or shameful; using technology in a completely secure way these days is all but impossible."



04-22-2015, 05:45 PM
Post: #7

cjpage2010
[nobody@HF:]

Prestige: 1
Posts: 26
Joined: Apr 2015
Reputation: 3

il buy them from you 5$ girls 1$ for guys, and im talking each

04-22-2015, 06:23 PM
Post: #8

Hopsin
who is omni
UB3R

Prestige: 477
Posts: 13,447
Joined: Dec 2010
Reputation: 882

There are several methods to earn money. Like mining, selling those slaves etc.

Quality > Quantity.

5$ girls 1$ for guys, and im talking each

IMAGE 04

• From hackforums.net. According to Hack Forums's own figures, the site contains 1,536,431 posts dedicated to acquiring, creating, and spreading RATs (as of 7/22/15).

STORIES OF CRUELTY—"RATS" ON THE ATTACK

Perhaps the best-known story of how RATs can put hopes and dreams in danger is the story of a California teen named Cassidy Wolf.

It started with Facebook. Cassidy Wolf remembers the first warning something was not right. "I went on to my Facebook and I had just like a notification on my home page telling me that someone from Utah had tried to log into my account," she said. "So when I saw that, I didn't think too much of it. I thought maybe it was just a malfunction. So I just changed my password."

That was on March 21, 2013, while Cassidy was spending an evening in Fullerton, California with friends. But in just about a half-hour, Cassidy would see similar warnings that someone was systematically changing her passwords on Facebook, Twitter, Instagram, Tumblr. Her social media profiles were lit on fire right in front of her eyes and there was nothing she could do to stop it. In a massive attack, a mysterious ratter made clear that he controlled much of the online world of the reigning Miss California Teen, Cassidy Wolf, just months before she competed in the Miss Teen USA pageant.

While this was the first time it was clear that her computer had been slaved, the hacker had control of Cassidy's computer for months. He'd been taking pictures of her changing clothes, listening to conversations, and monitoring emails. He now intended to use his collection of the private moments he had stolen from Cassidy.

Cassidy's mother Mary described the ratter's first email, which told Cassidy "do what I say or else I will post—and I don't remember if the word was hundreds, but there was a word there—I will post lots or tons of pictures and videos of you. And then as you scrolled down that's when the hair on the back of your neck went up. There were the pictures that were in the email. We could tell exactly they were (from) her bedroom."

The hacker would go onto threaten Cassidy, saying he wanted her to make a sexually explicit video. If she didn't comply, he said he would transform her "dream of being a model ... into [Cassidy being] a pornstar."[5]

Photograph by *GREG NELSEN*

IMAGE 05

- *Cassidy and Mary Wolf*

Cassidy did not give into the ratter's sextortion demands. Instead, she called the FBI. The ratter did post the photos, including one video designed to expose and humiliate Cassidy. His library of photos showed he spent time accumulating pictures and preparing his attack. When he didn't succeed, he hacked into her friends' accounts, urging them to pressure Cassidy to comply. This cyber stalker photoshopped her friends' faces onto pictures of naked women. One of the targets of his harassment was just 12 years old.

"I kinda had gotten the idea that this was gonna be my life forever," Cassidy said. "That I was gonna have this guy emailing me 40 times a day."

"I really didn't sleep for months," Mary Wolf said. "I thought he was coming because he kept saying it and his threats came around the clock. I didn't know if he lived down the block. I didn't know if it was somebody I was standing next to at the grocery store. We had no idea. I didn't know if it was a man, a woman, a child, you just couldn't tell."

The RAT knocked Cassidy offline briefly, but she didn't stay down. "At first, I deleted everything, I was scared and I thought I would never have my Twitter again, my Instagram, Facebook, I deleted seriously everything that I had online. And then I realized, why would I do that? Why would I give someone the power to take away something like that? Because for me my social media is really important, it helps with my job, its just really important as a public figure to have social media and I only saw it hurting me more by not having it. The first month, I was scared to use it. I was scared to go back on it when I first got it. Because I thought oh my gosh if this were to happen again I honestly don't know what I would do. Obviously I got over that and I realized that I was only giving him power by taking that away from me."

It took almost three months to capture Jared James Abrahams, a high school classmate. But Abrahams was more than a sick admirer of the girl with a locker down the hall. He, in fact, was "slaving" the devices of girls and young women around the world, with as many as 150 victims. Some were forced into recording sex acts while Abrahams commanded them to do his bidding.[6]

Cassidy Wolf first told her story publicly on the stage of the Miss Teen USA pageant. "I never posed for these pictures or purposely took these pictures, I was a victim in this situation. So I think that by speaking out about it, I didn't want to give Jared any power over my life. I didn't want to give him any satisfaction of seeing me hurt and seeing him take away any type of drive that I had towards my goals at the time. I just looked at it as I'm not gonna let this guy stop me and I'm gonna to stop him."

Mary Wolf had no idea Cassidy would tell her story to an international audience that evening. "At that moment, Cassidy was no longer a victim, she was now an advocate. She stood up and spoke out." She would win the title becoming Miss Teen USA 2013 and go on to talk about the experience with law enforcement, news outlets, and other young women.

In the summer of 2014, the FBI arrested nearly 100 hackers who used Blackshades, as were the two of the masterminds who developed the RAT. Did Cassidy's actions play a part in the arrests? Manhattan United States Attorney Preet Bharara told reporters who asked that question: "As is often true in other kinds of prosecutions and investigations, one successful investigation or prosecution leads to others."[7] It is impossible to know how many young women and girls are safer today because of Cassidy's voice.

"I think it is a very brave thing she did to stand up and admit to being a victim," said Georgia Weidman. "Victims feel rightly violated and often alone, thinking that their lives are over. Cassidy Wolf is beautiful and successful with a Wikipedia page about her accomplishment, and yet she went through this. I think it's important for victims to know that something like this doesn't have to define you or negatively impact the rest of your life."

For all his crimes, Abrahams is now serving an 18-month prison term. He'll be out this December. At some point soon, Jared James Abrahams will be back online.

Cassidy Wolf's story is painful to talk about, but in fact, there are thousands more stories like hers about which we never hear. That's because shame and fear keep the victims silent. The world would never know about these victims if not for law enforcement finding the photos. The investigators and prosecutors who work these cases are increasingly concerned about the rapid rise of ratters. We have three perspectives from people on the front lines of this fight against this insidious form of malware.

"RAT attacks on individuals are growing rapidly with more individuals who are knowledgeable about malware programs while brazen enough to use them," said Eimiller. "We've seen hundreds of victims in multiple cases just in Los Angeles. That's not including other federal offices, state, and local law enforcement. We're not going to arrest our way out of this problem, which is why educating parents and potential targets is important so that they avoid becoming victimized."

Scott Aken was an FBI cyber agent for more than five years. He said law enforcement doesn't have the resources to keep up with hackers, including the script kiddies using RATs. "Law enforcement just isn't equipped at this stage of the game to keep up with this stuff as fast as it's changing. People aren't trained enough. They don't have the manpower to go after the people that want to abuse the technology that was originally meant for good and is now being used for evil."

Wesley Hsu is the Chief of the Cyber and Intellectual Property Crimes Section of the U.S. Attorney's Office for the Central District of California in Los Angeles. His office has prosecuted several individuals accused of using RATs, including Luis Mijangos, who we will discuss more later in this report. Hsu said about RATs: "I think that it is something that we're going to see more and hopefully it's something that we can prosecute. But I think that RATs are an interesting tool because they allow the criminals to do any number of crimes. I mean we've talked about going after young women and their computers but you know the sky's the limit for the types of cases that a RAT can be used in."

The observations of victims, lawmakers, and white hat and black hat hackers alike convince us slaving is increasingly prevalent and dangerous. With a sense of the scope of the problem, we went looking for places where ratters hone and practice their craft. We found ratters utilizing two tools above all others—YouTube and content theft sites.

YOUTUBE HAS A RAT PROBLEM

It is easy to search YouTube to find thousands of videos, which offer:

- tutorials on how to use RATs and spread them to other devices;
- examples of successfully deployed RATs, with the faces and IP addresses of victims; and,
- links for ratters to download RATs they can use to slave devices.

And yes, many of these videos come with advertising running alongside them—meaning YouTube, or Google, is making money and then in some cases sharing it with ratters who proselytize their culture of creepy.

Researchers scoured hundreds of tutorial videos on YouTube, finding many with ratters demonstrating how they invade bedrooms and/or frighten young children. Ratters use YouTube to post their successful conquests for others to view, much the way a hunter hangs the head of their prey atop the fireplace.

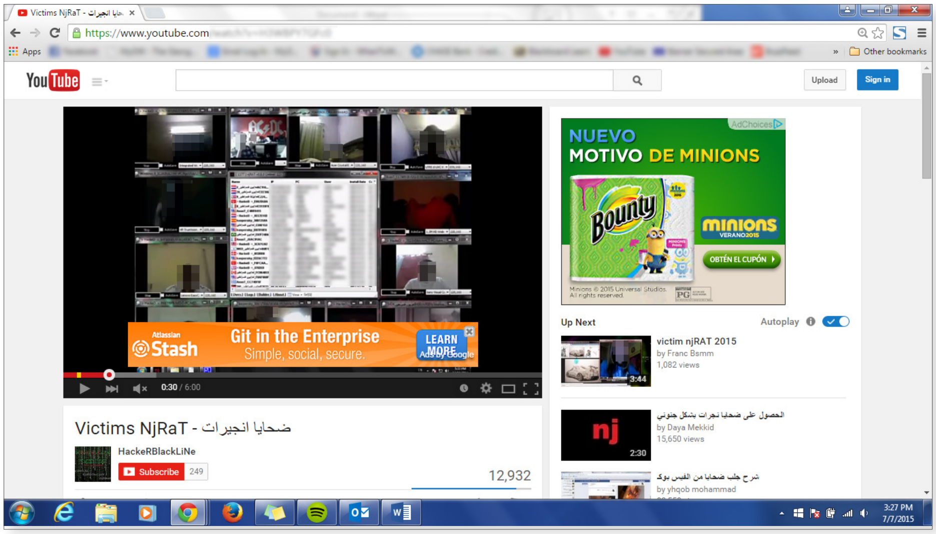
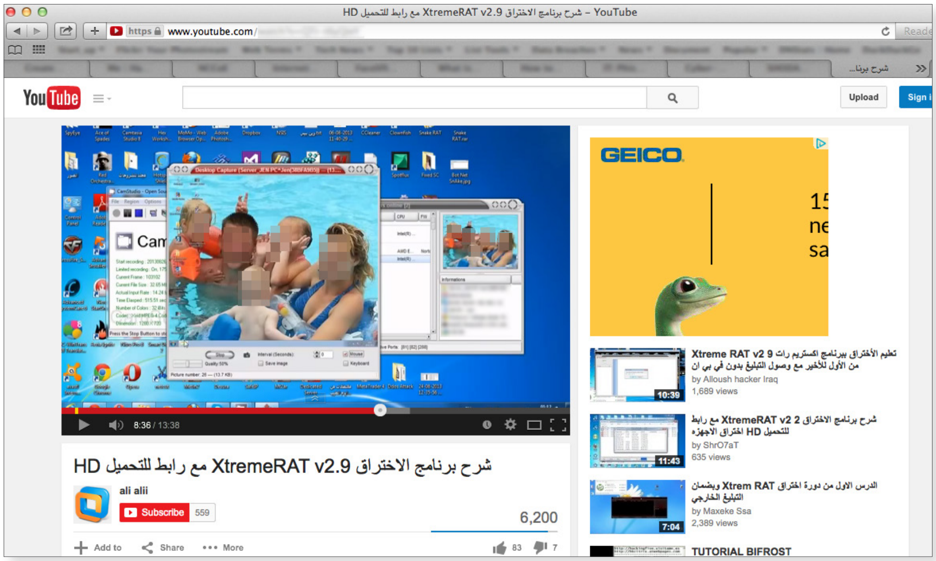


IMAGE 06

• At the time of this screenshot, this video had 12,932 views.



شرح برنامج الاختراق XtremeRAT v2.9 مع رابط للتحميل HD – YouTube
www.youtube.com
شرح برنامج الاختراق XtremeRAT v2.9 مع رابط للتحميل HD
ali alii
Subscribe 559
6,200
8:36 / 13:38
Add to
Share
More
83
7
GEICO
Xtreme RAT v2 9 تعليم الأختراق ببرنامج اكستريم رات
by Alloush hacker Iraq
1,689 views
شرح برنامج الاختراق XtremeRAT v2 2 مع رابط للتحميل HD اختراق الأجهزة
by ShrO7aT
635 views
الدرس الاول من دورة اختراق Xtrem RAT ويشمل التلبيق الخارجي
by Maxeke Ssa
2,389 views
TUTORIAL BIFROST

IMAGE 07

• At the time of this screenshot, this video had 6,200 views.

Many of these videos include other on-screen captions or an additional audio track from the ratters themselves as they celebrate their conquests, openly laughing and mocking the families they've frightened with scary voices or unexpected visuals.

The perpetrators of these scares want to terrorize their victims and then gloat about how they freaked out families. Nate Anderson, deputy editor of Ars Technica, described one video he found of a woman who left her computer on while feeding her baby. Anderson watched the ratters figure out how to interrupt and terrify the young mother as

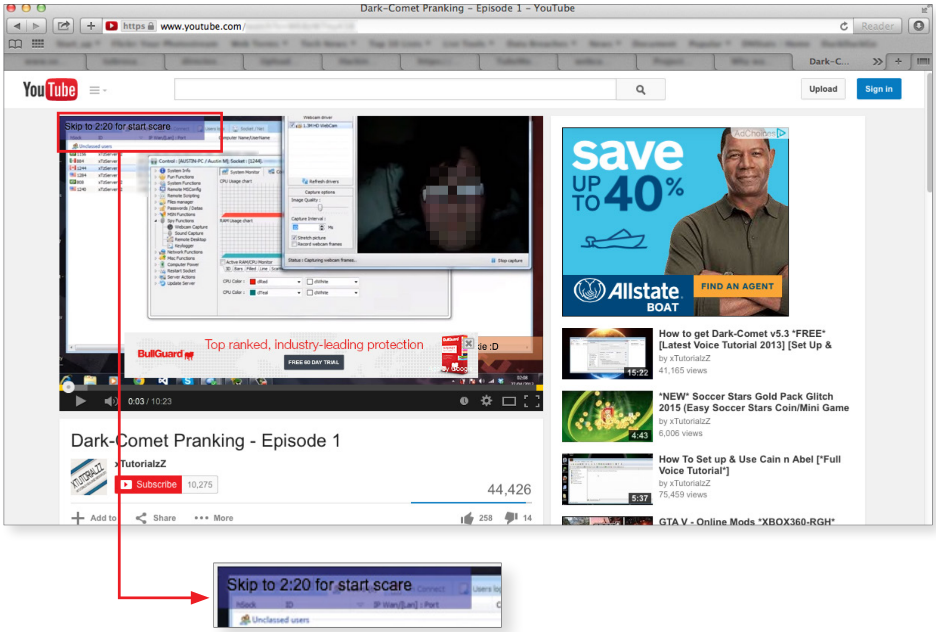
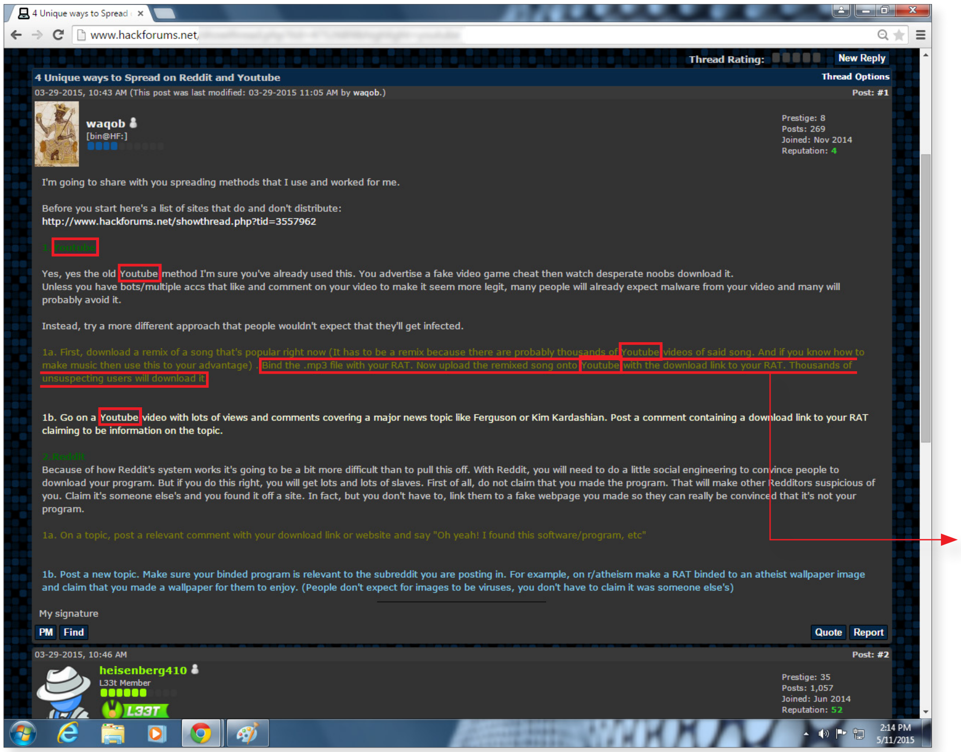

Dark-Comet Pranking – Episode 1 – YouTube
www.youtube.com
Skip to 2:20 for start scare
Top ranked, industry-leading protection
BullGuard
save UP TO 40%
Allstate BOAT
FIND AN AGENT
0:03 / 10:23
Dark-Comet Pranking - Episode 1
xTutorialzZ
Subscribe 10,275
44,426
How to get Dark-Comet v5.3 *FREE* [Latest Voice Tutorial 2013] [Set Up &
by xTutorialzZ
41,165 views
NEW Soccer Stars Gold Pack Glitch 2015 (Easy Soccer Stars Coin/Mini Game
by xTutorialzZ
6,006 views
How To Set up & Use Cain n Abel [*Full Voice Tutorial*]
by xTutorialzZ
75,459 views
GTA V - Online Mods *XBOX360-RGH*
Skip to 2:20 for start scare

IMAGE 08

• This video directs viewers to the time code where the "scare" of the RAT victim begins (highlighted).

• At the time of this screenshot, this video had 44,426 views.



4 Unique ways to Spread on Reddit and Youtube

03-29-2015, 10:43 AM (This post was last modified: 03-29-2015 11:05 AM by waqob.) Post: #1

waqob
[bin@HF:]

Prestige: 8
Posts: 269
Joined: Nov 2014
Reputation: 4

I'm going to share with you spreading methods that I use and worked for me.

Before you start here's a list of sites that do and don't distribute:
http://www.hackforums.net/showthread.php?tid=3557962

1. Youtube

Yes, yes the old Youtube method I'm sure you've already used this. You advertise a fake video game cheat then watch desperate noobs download it.
Unless you have bots/multiple accs that like and comment on your video to make it seem more legit, many people will already expect malware from your video and many will probably avoid it.

Instead, try a more different approach that people wouldn't expect that they'll get infected.

1a. First, download a remix of a song that's popular right now (It has to be a remix because there are probably thousands of Youtube videos of said song. And if you know how to make music then use this to your advantage) . Bind the .mp3 file with your RAT. Now upload the remixed song onto Youtube with the download link to your RAT. Thousands of unsuspecting users will download it.

1b. Go on a Youtube video with lots of views and comments covering a major news topic like Ferguson or Kim Kardashian. Post a comment containing a download link to your RAT claiming to be information on the topic.

2.Reddit
Because of how Reddit's system works it's going to be a bit more difficult than to pull this off. With Reddit, you will need to do a little social engineering to convince people to download your program. But if you do this right, you will get lots and lots of slaves. First of all, do not claim that you made the program. That will make other Redditors suspicious of you. Claim it's someone else's and you found it off a site. In fact, but you don't have to, link them to a fake webpage you made so they can really be convinced that it's not your program.

1a. On a topic, post a relevant comment with your download link or website and say "Oh yeah! I found this software/program, etc"

1b. Post a new topic. Make sure your binded program is relevant to the subreddit you are posting in. For example, on r/atheism make a RAT binded to an atheist wallpaper image and claim that you made a wallpaper for them to enjoy. (People don't expect for images to be viruses, you don't have to claim it was someone else's)

My signature

03-29-2015, 10:46 AM Post: #2

heisenberg410
L33t Member
L33T

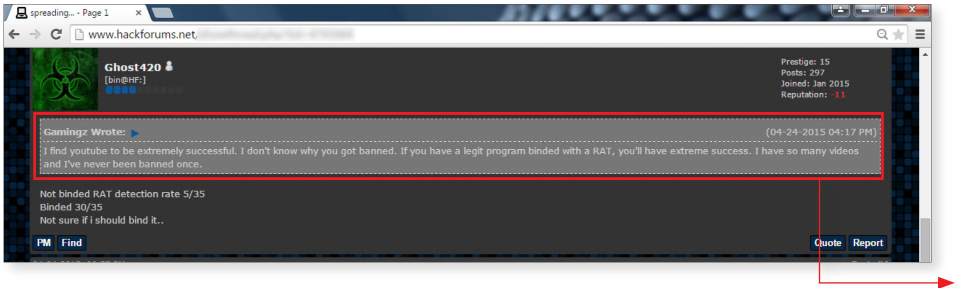
Prestige: 35
Posts: 1,057
Joined: Jun 2014
Reputation: 52

2:14 PM
5/11/2015

IMAGE 09

• From hackforums.net. This chat room for hackers has more than 2.8 million registered members (as of 7/22/15).

***• This portion below comes from a Hack Forums exchange titled "4 Unique ways to Spread on Reddit and Youtube."** One of the suggestions from the ratter, wagob, offers tips on how to use mp3 files shared in a post on YouTube: "Bind the .mp3 file with your RAT. Now upload the remixed song onto YouTube with the download link to your RAT. Thousands of unsuspecting users will download it."*



Ghost420
[bin@HF:]

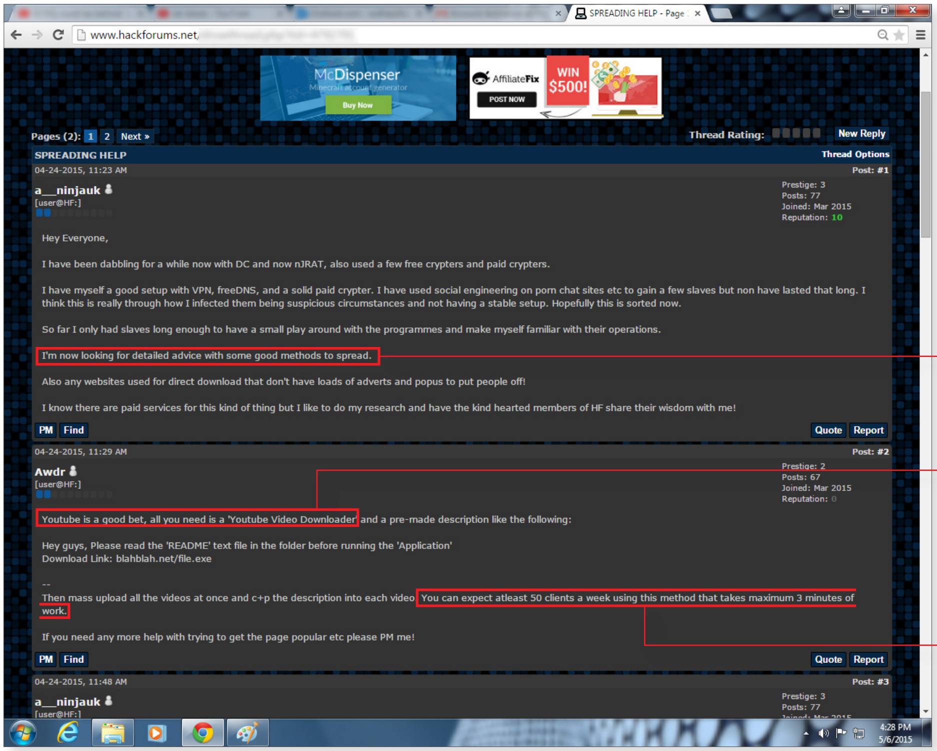
Prestige: 15
Posts: 297
Joined: Jan 2015
Reputation: -11

Gamingz Wrote: (04-24-2015 04:17 PM)
I find youtube to be extremely successful. I don't know why you got banned. If you have a legit program binded with a RAT, you'll have extreme success. I have so many videos and I've never been banned once.

Not binded RAT detection rate 5/35
Binded 30/35
Not sure if i should bind it..

IMAGE 10

- From hackforums.net.
- "Gamingz Wrote: I find youtube to be extremely successful. I don't know why you got banned. If you have a legit program bonded with a RAT, you'll have extreme success. I have so many videos and I've never been banned once."



SPREADING HELP

04-24-2015, 11:23 AM Post: #1

a__ninjauk
[user@HF:]

Prestige: 3
Posts: 77
Joined: Mar 2015
Reputation: 10

Hey Everyone,

I have been dabbling for a while now with DC and now nJRAT, also used a few free crypters and paid crypters.

I have myself a good setup with VPN, freeDNS, and a solid paid crypter. I have used social engineering on porn chat sites etc to gain a few slaves but non have lasted that long. I think this is really through how I infected them being suspicious circumstances and not having a stable setup. Hopefully this is sorted now.

So far I only had slaves long enough to have a small play around with the programmes and make myself familiar with their operations.

I'm now looking for detailed advice with some good methods to spread.

Also any websites used for direct download that don't have loads of adverts and popus to put people off!

I know there are paid services for this kind of thing but I like to do my research and have the kind hearted members of HF share their wisdom with me!

04-24-2015, 11:29 AM Post: #2

Awdr
[user@HF:]

Prestige: 2
Posts: 67
Joined: Mar 2015
Reputation: 0

Youtube is a good bet, all you need is a 'Youtube Video Downloader' and a pre-made description like the following:

Hey guys, Please read the 'README' text file in the folder before running the 'Application'
Download Link: blahblah.net/file.exe

--
Then mass upload all the videos at once and c+p the description into each video You can expect atleast 50 clients a week using this method that takes maximum 3 minutes of work.

If you need any more help with trying to get the page popular etc please PM me!

04-24-2015, 11:48 AM Post: #3

a__ninjauk
[user@HF:]

Prestige: 3
Posts: 77

IMAGE 11

- From hackforums.net.
- ***The portions below were taken from a Hack Forums exchange titled "SPREADING HELP."***

a____ninjauk: "I'm now looking for detailed advice with some good methods to spread."

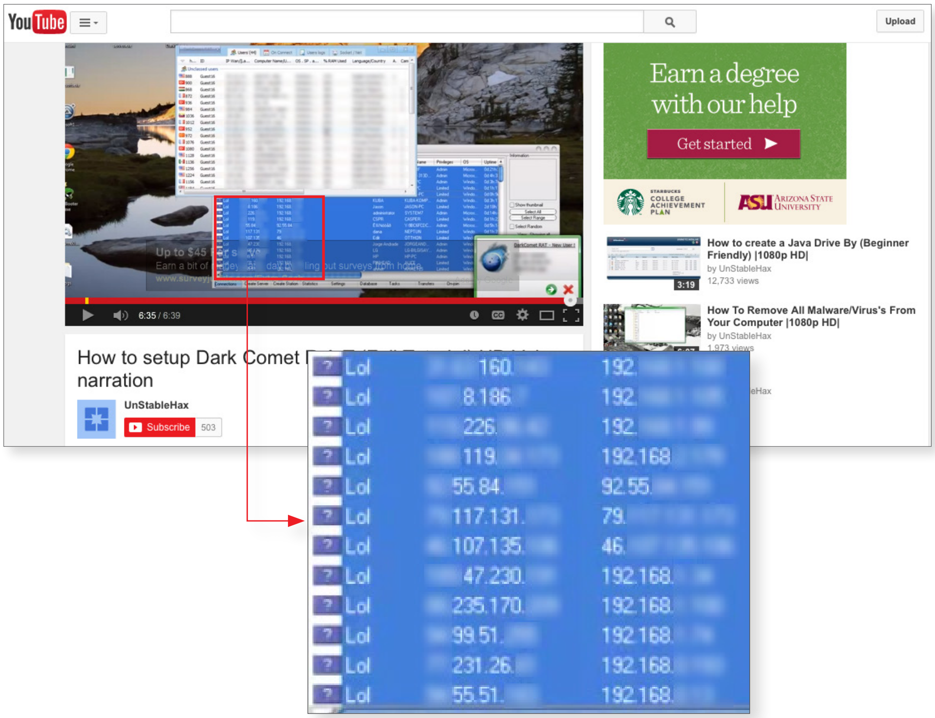
Awdr: YouTube is a good bet, all you need is a 'Youtube Video Downloader'...

Awdr: You can expect at least 50 clients a week using this method that takes maximum 3 minutes of work.

they flashed bizarre and disturbing images on her computer. In his story, Anderson wrote: "Copies of the incident aren't hard to find. They're on YouTube, along with thousands of other videos showing RAT controllers . . . pranking, or toying with victims."[8]

It is no secret amongst ratters. Researchers found plenty of examples of ratters discussing on Hack Forums how easy it is to spread RATs through YouTube.

Digital Citizens researchers found dozens of YouTube videos demonstrating ratters at work. Many of the videos included a ratter's control center with the IP addresses of slaved devices. YouTube videos provide the IP addresses of any number of devices around the world. Hackers can scroll through these lists almost like a menu of vulnerable people. On YouTube, these consumers are reduced to programming—or another vehicle for advertising revenue. This sharing between hackers is like thieves passing around a road map to houses that leave their back doors open.


YouTube
Upload
Earn a degree with our help
Get started ▶
Starbucks College Achievement Plan
ASU Arizona State University
How to create a Java Drive By (Beginner Friendly) |1080p HD|
by UnStableHax
12,733 views
3:19
How To Remove All Malware/Virus's From Your Computer |1080p HD|
by UnStableHax
1,973 views
6:35 / 6:39
How to setup Dark Comet
narration
UnStableHax
Subscribe
503

Lol	160.	192.
Lol	8.186.	192.
Lol	226.	192.
Lol	119.	192.168.
Lol	55.84.	92.55.
Lol	117.131.	79.
Lol	107.135.	46.
Lol	47.230.	192.168.
Lol	235.170.	192.168.
Lol	99.51.	192.168.
Lol	231.26.	192.168.
Lol	55.51.	192.168.

IMAGE 12

• In this tutorial, you can find IP addresses for computers in countries around the world, including devices located in the United States, Turkey, France, and Mexico. The video includes an ad for Starbucks.

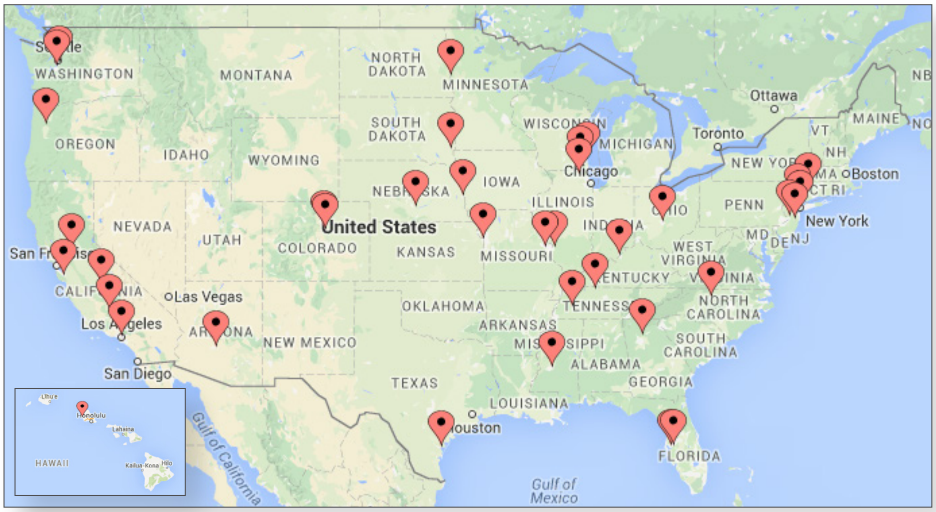


IMAGE 13

• This is a map of US cities with slaved devices shared on YouTube videos accompanied by advertising. For a list of these cities, as well as a map of slaved devices found in videos without ads, see Appendix B.

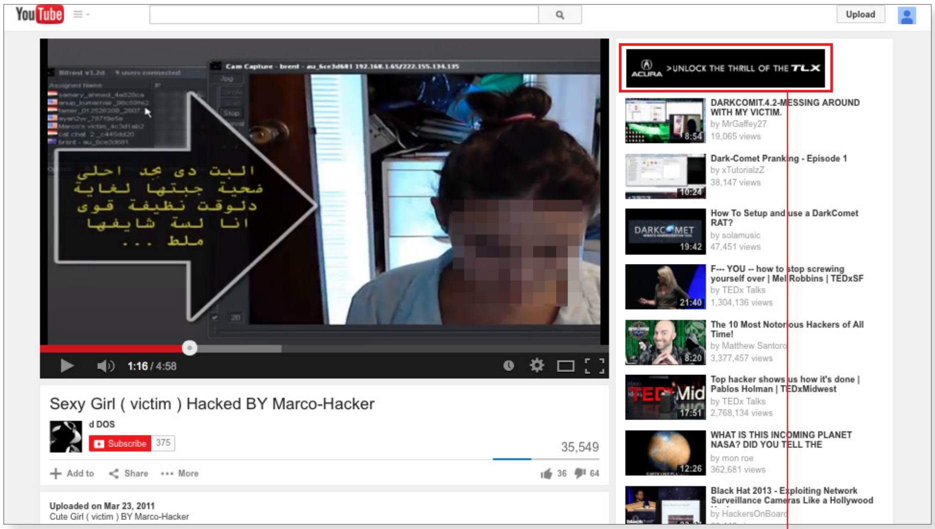
Our researchers pinpointed the IPs exposed on YouTube to devices in cities across America.[d] As you can see in image 13, America has a growing RAT infestation problem.

Sadly, people are coming to these pages. Our researchers found many videos with tens of thousands of views; particularly popular were those that included a picture of a victim—like the screenshot we included at the beginning of this report.

[d] Using the websites IP location (www.iplocation.net) and Network Solutions (www.networksolutions.com/), Digital Citizens researchers determined the current locations of devices with the IP numbers shared in RAT tutorials now on YouTube. The IP location tools tell our researchers where the IP addresses were located as of the time of the research, not necessarily at the time the video was posted. If you move or get a new device from an ISP, it is possible your IP address will change. For this reason, we didn't use IP numbers from videos posted before 2013. However, in any case, once a RAT infects your system, the system will try to connect back to the hacker's system using any IP address that is on the Internet. The geographical location of IP addresses is imperfect and can be masked.

"There will be more pins on the map unless companies change their moral compass and take steps to stop the sharing of these crime videos," said Hemanshu Nigam, Chief Executive Officer of SSP Blue and a former federal prosecutor against online child and computer crimes for the U.S. Department of Justice. "Those pins are people and some of them may not even be aware of how often they are being victimized. These innocent victims are mining bitcoins or launching DDoS attacks or pushing RATs to their neighbors. We must take a stand as an industry and as a society to prevent anyone from profiting from this digital rape."

It was that video that haunted us more than any other. It included several U.S. IPs, but it was the face in the picture that concerned us the most. That YouTube video, titled "Sexy Girl (victim) Hacked BY Marco-Hacker" shows her working on a class paper in what looks like a bedroom, with no idea she is being watched. From her IP address, we determined she was likely in Australia. We can also see the ratter is using "Bifrost", a well-known RAT, to access her computer.



Sexy Girl (victim) Hacked BY Marco-Hacker

d DOS

375

35,549

36 64

Uploaded on Mar 23, 2011
Cute Girl (victim) BY Marco-Hacker

DARKCOMIT.4.2-MESSING AROUND WITH MY VICTIM.
by MrGaffey27
19,065 views
8:54

Dark-Comet Pranking - Episode 1
by xTutorialzZ
38,147 views
10:24

How To Setup and use a DarkComet RAT?
by solamusic
47,451 views
19:42

F--- YOU -- how to stop screwing yourself over | Mel Robbins | TEDxSF
by TEDx Talks
1,304,136 views
21:40

The 10 Most Notorious Hackers of All Time!
by Matthew Santoro
3,377,457 views
8:20

Top hacker shows us how it's done | Pablos Holman | TEDxMidwest
by TEDx Talks
2,768,134 views
17:51

WHAT IS THIS INCOMING PLANET NASA? DID YOU TELL THE
by mon roe
362,681 views
12:26

Black Hat 2013 - Exploiting Network Surveillance Cameras Like a Hollywood
by HackersOnBoard

IMAGE 14

• Digital Citizens researchers found ads for Acura, American Express, and other well-known, trusted brands in late 2014 and early 2015.

With the help of the translation service TransPerfect, Digital Citizens did get a translation of the discussion in the YouTube video:

TIME CODE	ARABIC TRANSCRIPTION	ENGLISH TRANSLATION
0:58	هههه لص شكله ده الواد	This guy looks like a thief hahahaha (laughing sound).
1:15	لغاية جبتها ضحية احلى بجد دي البت ملط شايفها لسة أنا قوي نظيفة دلوقت	This girl is seriously the most beautiful victim I've had so far. She is quite clean, I just saw her naked.
2:08	اللي ايه ملط يكون لما دة الجسم تتخيلوا يعمله المفروض الواحد	Imagine when a body like that is naked, what is the guy supposed to do.
2:55	ههههههههه ليه مزهولة هي أعرف نفسي	I wish I know why she looks so astonished . . . hahahahahahaha (laughing sound).

The rest of the translation included crude sexual commentary. Nigam said about the video: "This is digital rape. This is a violation of her rights and allowing it to be shown over and over is re-victimizing her repeatedly in front of the eyes of the world."

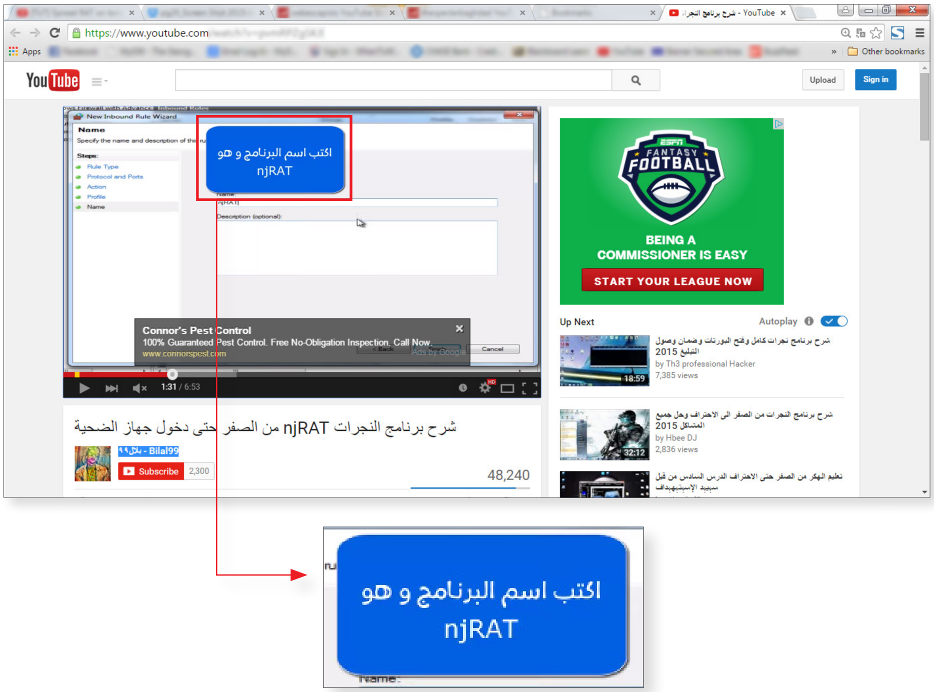
Digital Citizens shared the information about this video with a respected child safety organization to ascertain if there is a threat to the girl and her family. The video came down in March of this year, nearly four years after it was posted.

Advertising running alongside these ratter videos is a common practice. Our researchers searched YouTube using the term "how to download and use ____RAT." We filled in the blank with five of the most recognized RATs—Bifrost, Blackshades, DarkComet, njRAT, and Poison Ivy. We got 30,490 hits. To be fair, some of those items include news stories on RATs and other items. We went through the first two pages of search results for each query to see how many videos were "valid", or videos that actually demonstrated what we searched for—how to download and use ____RAT. Once we eliminated the invalid videos, we looked at how many valid videos have ads. In all, 38 percent of the valid RAT videos had some advertising running alongside the video (to see the details on this search, go to Appendix C).

To put that in perspective, 38 percent of 30,490 is 11,586. You would have to watch every hour of network programming on a broadcast channel for 34 days to view 11,586 ads.[9]

Companies like Acura and American Express pay YouTube's parent company Google for ad space. Not all YouTube videos have advertising. Ads show up when the "poster" of the video has signed up for the YouTube Partner Program, which makes them eligible to get a cut of whatever ad revenue is generated from views of the video. In this case, the person who posted their invasion of this girl's bedroom gets a portion of whatever Acura, American Express, and other advertisers paid to purchase the ad space.

As we looked through hundreds of RAT videos, we found ads for respected, premium brands like Procter & Gamble, Wells Fargo, and Boeing running alongside videos showing the faces of victims; we even found ads for baseball tickets to New York Yankees games next to tutorials.



شرح برنامج النجرا - YouTube

https://www.youtube.com

New Inbound Rule Wizard

Name

Specify the name and description of this ru

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

اكتب اسم البرنامج و هو njRAT

Name:

njRAT|

Description (optional):

Connor's Pest Control
100% Guaranteed Pest Control. Free No-Obligation Inspection. Call Now.
www.connorspest.com
Ads by Google

1:31 / 6:53

شرح برنامج النجرات njRAT من الصفر حتى دخول جهاز الضحية

بلال٩٩ - Bilal99

Subscribe 2,300

48,240

BEING A COMMISSIONER IS EASY

START YOUR LEAGUE NOW

Up Next — Autoplay

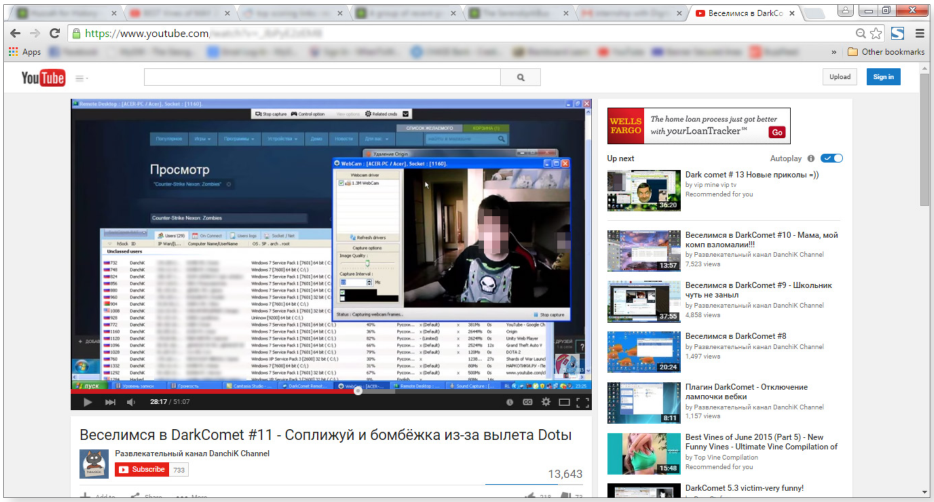
شرح برنامج نجرات كامل وفتح البورتات وضمان وصول التبليغ 2015
by Th3 professional Hacker
7,385 views

شرح برنامج النجرات من الصفر الى الاحتراف وحل جميع المشاكل 2015
by Hbee DJ
2,836 views

تعليم الهكر من الصفر حتى الاحتراف الدرس السادس من قبل سبيبد الإسبتهيهدف

IMAGE 15

- njRAT demonstration in Arabic with an ESPN Fantasy Football ad.
- At the time of this screenshot, this video had 48,240 views.



Веселимся в DarkCo

https://www.youtube.com

Просмотр

"Counter-Strike Nexon: Zombies"

WebCam : [ACER-PC / Acer], Socket : [1160].

Status : Capturing webcam frames...

28:17 / 51:07

Веселимся в DarkComet #11 - Соплижуй и бомбёжка из-за вылета Dotы

Развлекательный канал DanchiK Channel

Subscribe 733

13,643

WELLS FARGO The home loan process just got better with yourLoanTracker℠ Go

Up next — Autoplay

Dark comet # 13 Новые приколы =))
by vip mine vip tv
Recommended for you

Веселимся в DarkComet #10 - Мама, мой комп взломали!!!
by Развлекательный канал DanchiK Channel
7,523 views

Веселимся в DarkComet #9 - Школьник чуть не заныл
by Развлекательный канал DanchiK Channel
4,858 views

Веселимся в DarkComet #8
by Развлекательный канал DanchiK Channel
1,497 views

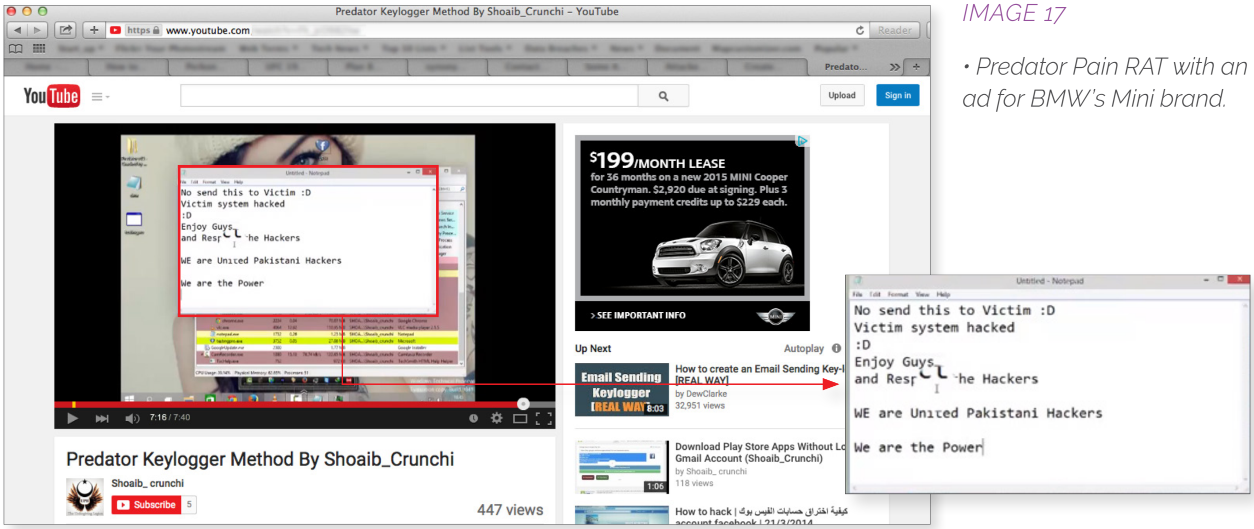
Плагин DarkComet - Отключение лампочки вебки
by Развлекательный канал DanchiK Channel
1,157 views

Best Vines of June 2015 (Part 5) - New Funny Vines - Ultimate Vine Compilation of
by Top Vine Compilation
Recommended for you

DarkComet 5.3 victim-very funny!

IMAGE 16

- DarkComet demonstration in Russian with an ad for Wells Fargo.
- At the time of this screenshot, this video had 13,643 views.



Predator Keylogger Method By Shoaib_Crunchi – YouTube

https www.youtube.com

```
No send this to Victim :D
Victim system hacked
:D
Enjoy Guys
and Resp  he Hackers

WE are United Pakistani Hackers

We are the Power
```

$199/MONTH LEASE for 36 months on a new 2015 MINI Cooper Countryman. $2,920 due at signing. Plus 3 monthly payment credits up to $229 each.

> SEE IMPORTANT INFO

Up Next — Autoplay

How to create an Email Sending Key-l [REAL WAY] by DewClarke 32,951 views 8:03

Download Play Store Apps Without Lo Gmail Account (Shoaib_Crunchi) by Shoaib_ crunchi 118 views 1:06

How to hack | كيفية اختراق حسابات الفيس بوك account facebook | 21/3/2014

7:16 / 7:40

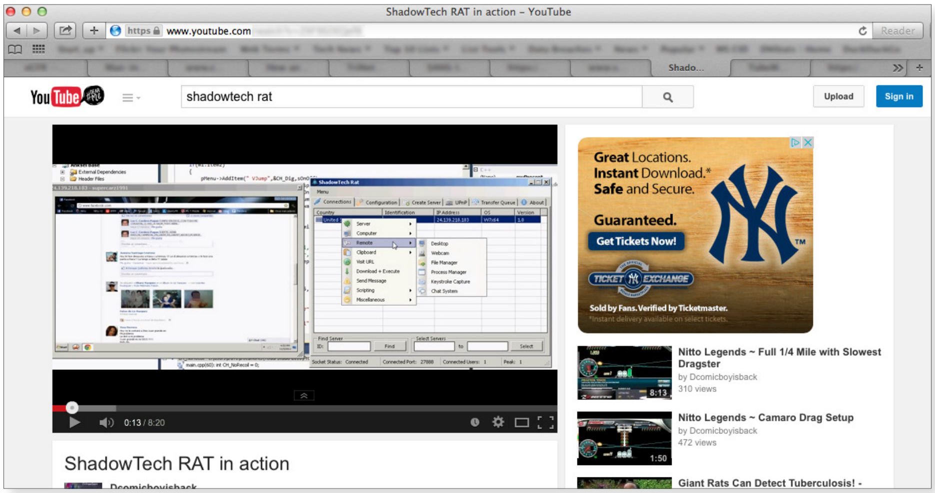
Predator Keylogger Method By Shoaib_Crunchi

Shoaib_ crunchi — Subscribe 5 — 447 views

Predato...
Upload
Sign in
Reader
Email Sending Keylogger [REAL WAY]
Untitled - Notepad
File Edit Format View Help

IMAGE 17

- Predator Pain RAT with an ad for BMW's Mini brand.



ShadowTech RAT in action – YouTube

https www.youtube.com

shadowtech rat

Great Locations. Instant Download.* Safe and Secure. Guaranteed. Get Tickets Now!

TICKET EXCHANGE

Sold by Fans. Verified by Ticketmaster.

*Instant delivery available on select tickets.

Nitto Legends ~ Full 1/4 Mile with Slowest Dragster by Dcomicboyisback 310 views 8:13

Nitto Legends ~ Camaro Drag Setup by Dcomicboyisback 472 views 1:50

Giant Rats Can Detect Tuberculosis! -

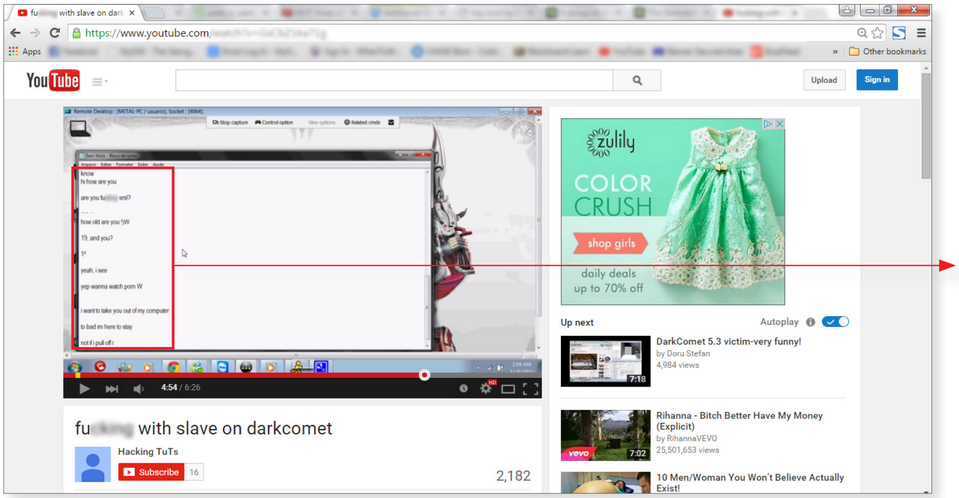
0:13 / 8:20

ShadowTech RAT in action

Dcomicboyisback

IMAGE 18

- ShadowTech RAT demonstration with an ad for New York Yankees tickets.



fu[redacted] with slave on dark

https://www.youtube.com

Remote Desktop : [METAL-PC / usuario], Socket : [4064].

Stop capture — Control option — View options — Related cmds

zulily COLOR CRUSH shop girls daily deals up to 70% off

Up next — Autoplay

DarkComet 5.3 victim-very funny! by Doru Stefan 4,984 views 7:18

Rihanna - Bitch Better Have My Money (Explicit) by RihannaVEVO 25,501,653 views 7:02

10 Men/Woman You Won't Believe Actually Exist!

4:54 / 6:26

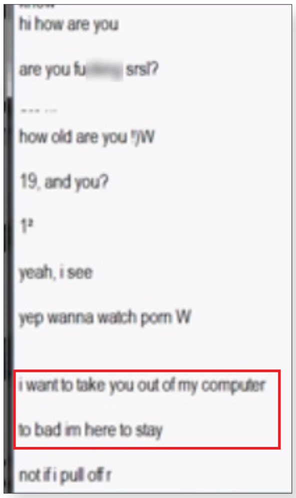
fu[redacted] with slave on darkcomet

Hacking TuTs — Subscribe 16 — 2,182

Apps
Other bookmarks
Upload
Sign in
Sem título - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda

IMAGE 19

- DarkComet RAT demonstration with conversation between ratter and victim and an ad for Zulily.



hi how are you

are you fu[redacted] srsl?

how old are you ?W

19, and you?

1²

yeah, i see

yep wanna watch porn W

i want to take you out of my computer

to bad im here to stay

not if i pull off r

When we first showed the YouTube screenshots we found to Cassidy Wolf, she said:

> "This could have been my face blurred out . . . . and it's sad because they seriously have no idea. I mean I had not one clue of having someone watching me. It never passed my mind for the entire year."

And when we asked about the advertising running alongside the videos marketing and demonstrating how RATs can be used, she added: "I think it's crazy that it's now a world where people can make money off it." She said Google should go after ratters videos on YouTube the same way the company has gone after child pornography and human trafficking: "I think Google should make it just as high a priority as it is with any other type of criminal activity."

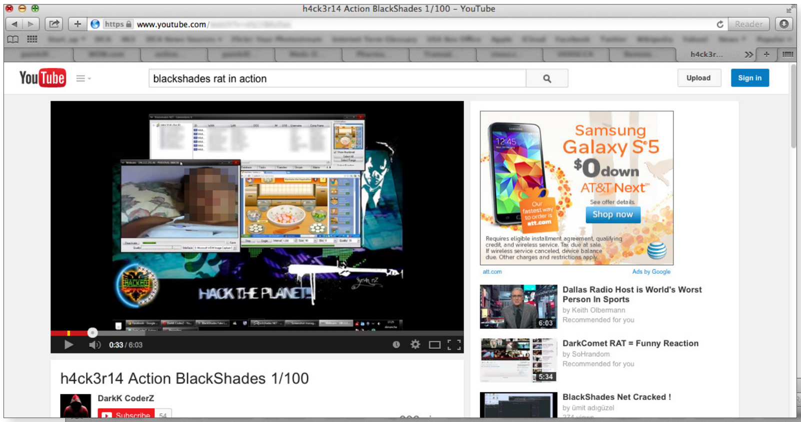

h4ck3r14 Action BlackShades 1/100 – YouTube
www.youtube.com
Reader
h4ck3r...
YouTube
blackshades rat in action
Upload
Sign in
HACK THE PLANET
0:33 / 6:03
h4ck3r14 Action BlackShades 1/100
DarkK CoderZ
Subscribe
Samsung Galaxy S5
$0down
AT&T Next
See offer details.
Shop now
Our fastest way to order is att.com
Requires eligible installment agreement, qualifying credit, and wireless service. Tax due at sale. If wireless service canceled, device balance due. Other charges and restrictions apply.
att.com
Ads by Google
Dallas Radio Host is World's Worst Person In Sports
by Keith Olbermann
Recommended for you
6:03
DarkComet RAT = Funny Reaction
by SoHrandom
Recommended for you
5:34
BlackShades Net Cracked !
by ümit adıgüzel

IMAGE 20

• *Blackshades demonstration with an AT&T ad for the Samsung Galaxy S5.*

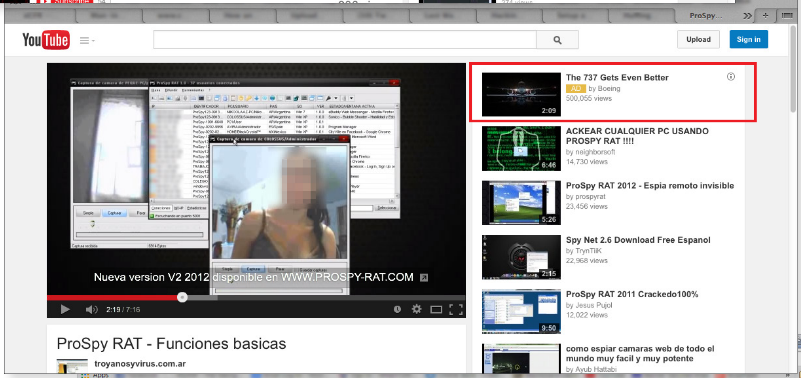

ProSpy...
YouTube
Upload
Sign in
Nueva version V2 2012 disponible en WWW.PROSPY-RAT.COM
2:19 / 7:16
ProSpy RAT - Funciones basicas
troyanosyvirus.com.ar
The 737 Gets Even Better
AD by Boeing
500,055 views
2:09
ACKEAR CUALQUIER PC USANDO PROSPY RAT !!!!
by neighborsoft
14,730 views
6:46
ProSpy RAT 2012 - Espia remoto invisible
by prospyrat
23,456 views
5:26
Spy Net 2.6 Download Free Espanol
by TrynTiiK
22,968 views
2:15
ProSpy RAT 2011 Crackedo100%
by Jesus Pujol
12,022 views
9:50
como espiar camaras web de todo el mundo muy facil y muy potente
by Ayub Hattabi

IMAGE 21

• *ProSpy demonstration in Spanish with a Boeing ad.*

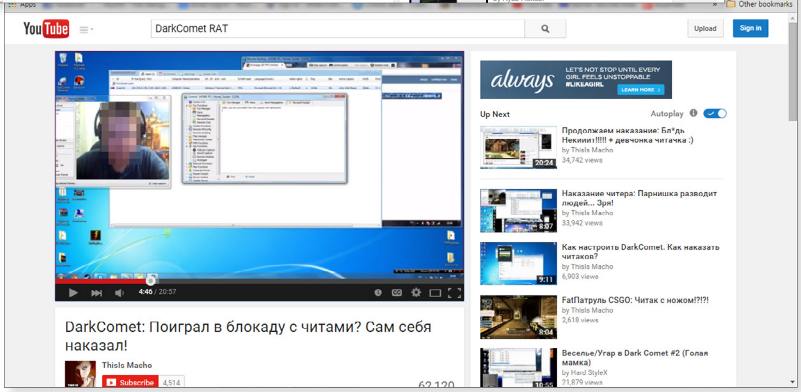

Other bookmarks
YouTube
DarkComet RAT
Upload
Sign in
4:46 / 20:57
DarkComet: Поиграл в блокаду с читами? Сам себя наказал!
ThisIs Macho
Subscribe
4,514
62,120
always
LET'S NOT STOP UNTIL EVERY GIRL FEELS UNSTOPPABLE
#LIKEAGIRL
LEARN MORE
Up Next
Autoplay
Продолжаем наказание: Бл*дь Некиииит!!!!! + девчонка читачка :)
by ThisIs Macho
34,742 views
20:24
Наказание читера: Парнишка разводит людей... Зря!
by ThisIs Macho
33,942 views
8:07
Как настроить DarkComet. Как наказать читаков?
by ThisIs Macho
6,903 views
9:11
FatПатруль CSGO: Читак с ножом!?!?!
by ThisIs Macho
2,618 views
8:04
Веселье/Угар в Dark Comet #2 (Голая мамка)
by Hard StyleX
21,879 views
10:55

IMAGE 22

• *DarkComet RAT demonstration in Russian with an ad for Procter & Gamble's Always feminine hygiene products.*

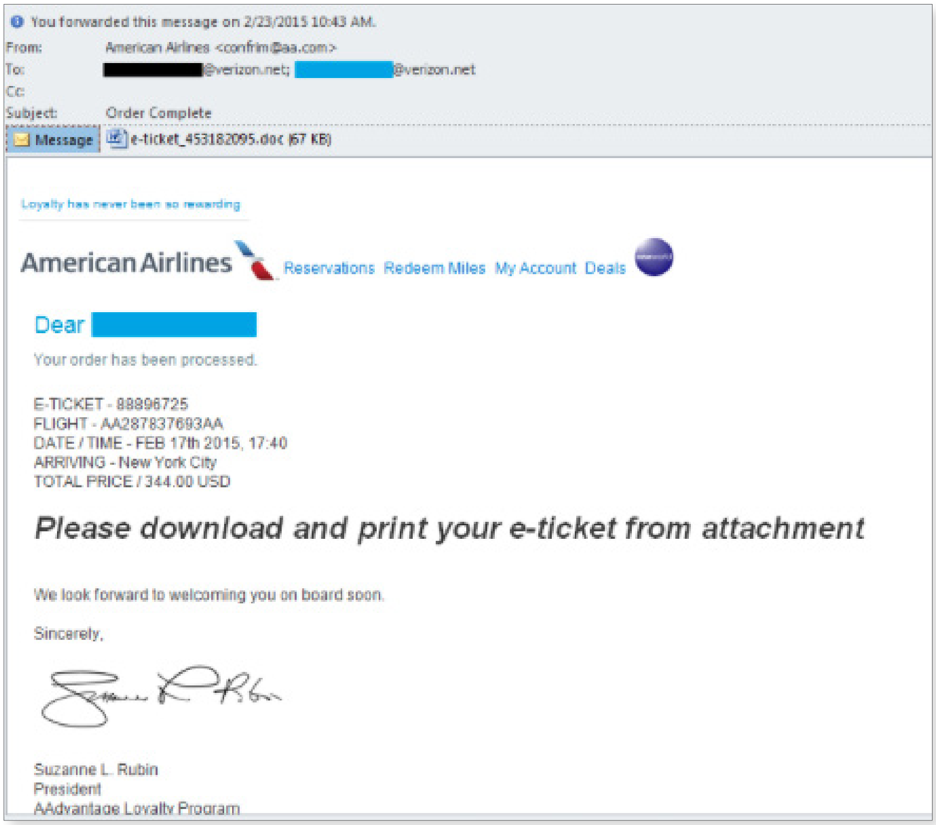
UNLEASHING A RAT—THE ART OF "SPREADING"

Launching a RAT is not just computer science; it is an art. There are tutorials about just the "spreading" of the malware. It takes several steps. The attack often begins with a well-crafted email making an offer that the victim can't refuse. The email is the launch of a "spear phishing" attack.

The sophistication of these emails has grown faster than awareness of their danger. Verizon researchers say phishing campaigns were more effective in 2014 than ever before. Looking at two recent security surveys in which a total of 150,000 test emails went out, researchers found that 50 percent of users opened the email and clicked on dangerous links—in just the first hour after sending.[10]

How do they do it? Spear phishers include a link or an attachment designed to get your click. It might include specific information, which is increasingly easier to find, to gain your trust. For example, look at the example below—an email one of our researchers received designed to look like an email from American Airlines.[e]

Mail like this, which appears to come from a trusted and respected brand, troubles security experts who say we've all become increasing comfortable with clicking on links and attachments: "Links are meant to be clicked. Many of us click on hundreds of links a week," said Megan Horner of Blackfin Security. "At this point, it goes against human nature. It gets hard to stop, even when you see something that should give you pause."



You forwarded this message on 2/23/2015 10:43 AM.

From: American Airlines <confrim@aa.com>

To: [redacted]@verizon.net; [redacted]@verizon.net

Cc:

Subject: Order Complete

Message | e-ticket_453182095.doc (67 KB)

Loyalty has never been so rewarding

American Airlines Reservations Redeem Miles My Account Deals

Dear [redacted]

Your order has been processed.

E-TICKET - 88896725
FLIGHT - AA287837693AA
DATE / TIME - FEB 17th 2015, 17:40
ARRIVING - New York City
TOTAL PRICE / 344.00 USD

Please download and print your e-ticket from attachment

We look forward to welcoming you on board soon.

Sincerely,

Suzanne L. Rubin
President
AAdvantage Loyalty Program

IMAGE 23

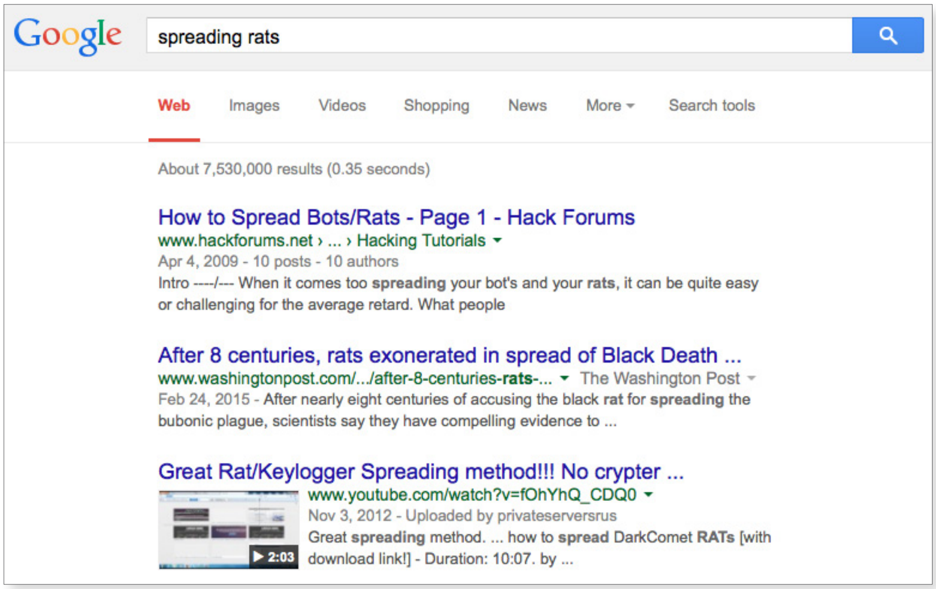
• This is an example of a spear phishing email—a fake American Airlines email, a flight confirmation sent to a Digital Citizens' researcher who had no travel plans. The researcher downloaded the attachment, then monitored it as an anti-virus application immediately caught and removed the Trojan from the system.

[e] To learn more about this email and spear phishing, go to: http://www.digitalcitizensalliance.org/cac/alliance/postdetailaspx?Id=240

For ratters, spear phishing emails are an easy way to launch an attack on victims. Consider the methods deployed by Luis Mijangos, one of the most vicious ratters on record. Mijangos was not like the high school student Jared James Abrahams—he was a skilled hacker who could build his own tools and spread them without consult or guidance. Mijangos used his skills to force, trick, or steal materials from 230 victims, including 44 juveniles.[11] He used Poison Ivy and SpyNet[12] to poach files from hard drives or take control of webcams to make sexually explicit videos. A skilled spear phisher, Mijangos knew it is not enough just to get into the inbox. He had to convince his target to click on something—an attachment, a link, an application—so his RAT would be downloaded onto the device. One of Mijangos' lures of choice was music downloads from peer-to-peer sites. According to Ars Technica, Mijangos "was seeding peer-to-peer networks with popular-sounding song titles that were actually malware."[13]

In *Digital Peepholes*, a research paper from IIT Chicago-Kent College of Law, examining the threat the hacking of webcams poses to privacy, legal scholars Lori Andrews, Michael Holloway, and Dan Massoglia reported that ratters disguise RATs as popular songs then upload them to torrent sites.[14] Is sharing links to content theft sites the top method for spreading rats? It is if you look at Google's search results. When we searched for "spreading rats" on Google on June 24, 2015, the first search result was a link to a chat on Hack Forums (see images 24 and 25).

We clicked on that link and found several posts directing potential ratters to use content theft sites.



About 7,530,000 results (0.35 seconds)

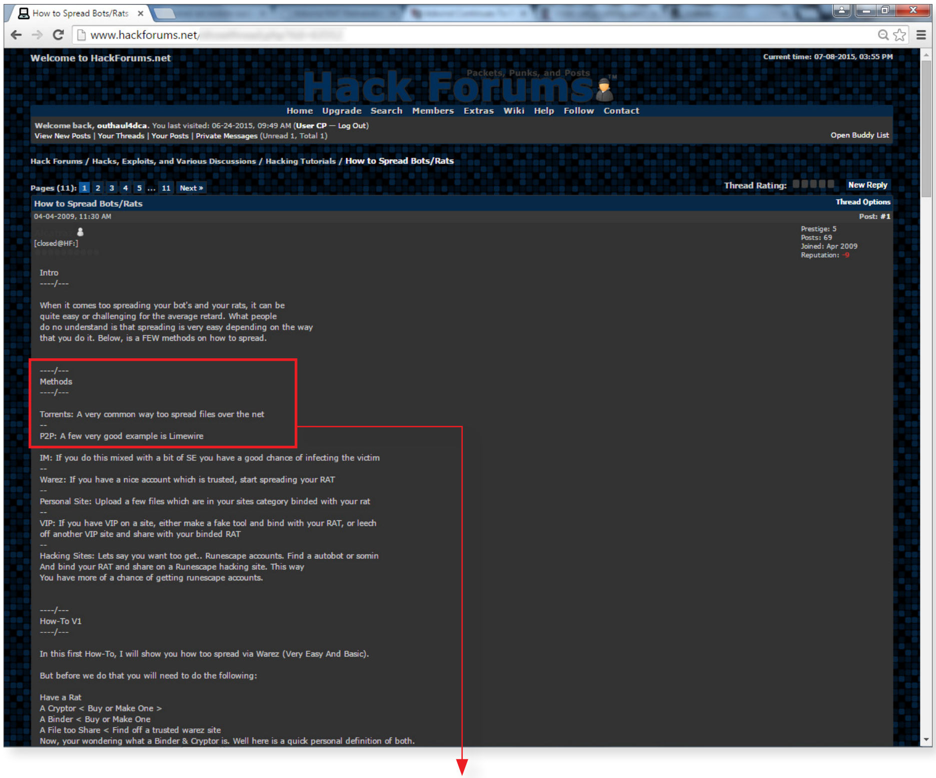
How to Spread Bots/Rats - Page 1 - Hack Forums
www.hackforums.net › ... › Hacking Tutorials
Apr 4, 2009 - 10 posts - 10 authors
Intro ----/--- When it comes too **spreading** your bot's and your **rats**, it can be quite easy or challenging for the average retard. What people

After 8 centuries, rats exonerated in spread of Black Death ...
www.washingtonpost.com/.../after-8-centuries-**rats**-... The Washington Post
Feb 24, 2015 - After nearly eight centuries of accusing the black rat for **spreading** the bubonic plague, scientists say they have compelling evidence to ...

Great Rat/Keylogger Spreading method!!! No crypter ...
www.youtube.com/watch?v=fOhYhQ_CDQ0
Nov 3, 2012 - Uploaded by privateserversrus
Great **spreading** method. ... how to **spread** DarkComet **RATs** [with download link!] - Duration: 10:07. by ...

IMAGE 24

• Page one of Google search results for "spreading rats" from June 24, 2015.


How to Spread Bots/Rats
www.hackforums.net/[redacted]
Welcome to HackForums.net
Current time: 07-08-2015, 03:55 PM
Hack Forums
Packets, Punks, and Posts
Home Upgrade Search Members Extras Wiki Help Follow Contact
Welcome back, outhaul4dca. You last visited: 06-24-2015, 09:49 AM (User CP — Log Out)
View New Posts | Your Threads | Your Posts | Private Messages (Unread 1, Total 1)
Open Buddy List
Hack Forums / Hacks, Exploits, and Various Discussions / Hacking Tutorials / How to Spread Bots/Rats
Pages (11): 1 2 3 4 5 ... 11 Next »
Thread Rating:
New Reply
Thread Options

How to Spread Bots/Rats
04-04-2009, 11:30 AM
Post: #1
[redacted]
[closed@HF:]
Prestige: 5
Posts: 69
Joined: Apr 2009
Reputation: -9

Intro
----/---

When it comes too spreading your bot's and your rats, it can be
quite easy or challenging for the average retard. What people
do no understand is that spreading is very easy depending on the way
that you do it. Below, is a FEW methods on how to spread.

----/---
Methods
----/---

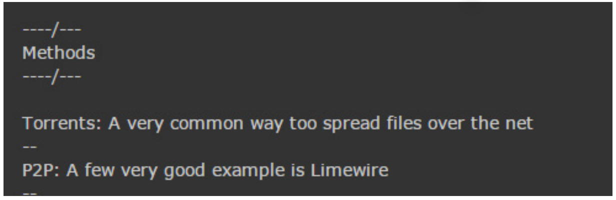
Torrents: A very common way too spread files over the net
--
P2P: A few very good example is Limewire
--
IM: If you do this mixed with a bit of SE you have a good chance of infecting the victim
--
Warez: If you have a nice account which is trusted, start spreading your RAT
--
Personal Site: Upload a few files which are in your sites category binded with your rat
--
VIP: If you have VIP on a site, either make a fake tool and bind with your RAT, or leech
off another VIP site and share with your binded RAT
--
Hacking Sites: Lets say you want too get.. Runescape accounts. Find a autobot or somin
And bind your RAT and share on a Runescape hacking site. This way
You have more of a chance of getting runescape accounts.

----/---
How-To V1
----/---

In this first How-To, I will show you how too spread via Warez (Very Easy And Basic).

But before we do that you will need to do the following:

Have a Rat
A Cryptor < Buy or Make One >
A Binder < Buy or Make One
A File too Share < Find off a trusted warez site
Now, your wondering what a Binder & Cryptor is. Well here is a quick personal definition of both.


----/---
Methods
----/---

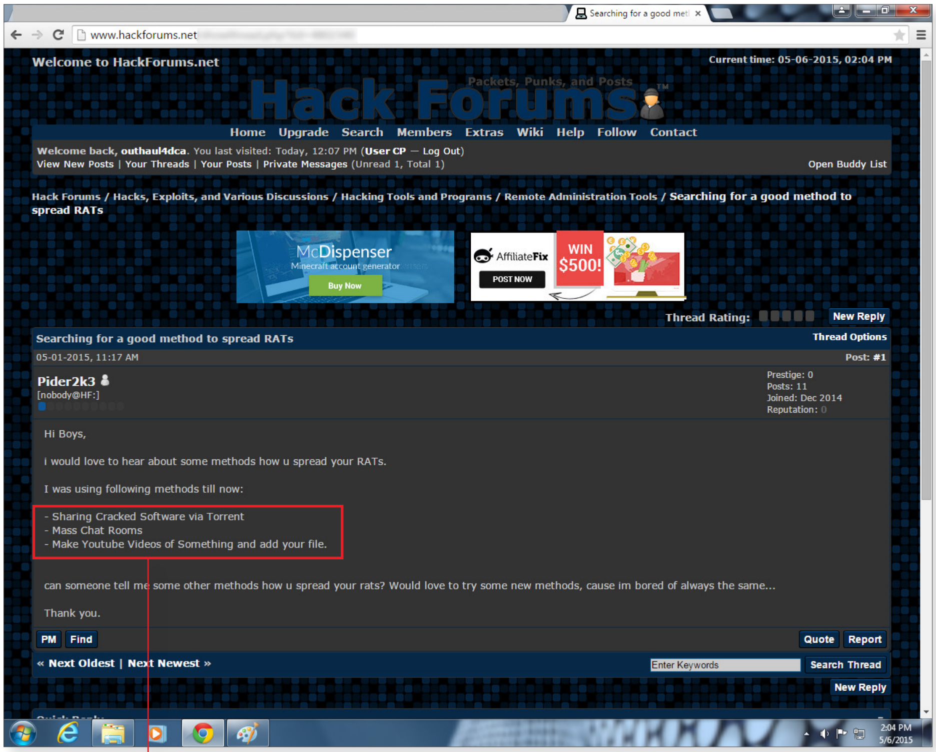
Torrents: A very common way too spread files over the net
--
P2P: A few very good example is Limewire
--

IMAGE 25

• From the hackers' chat room, hackforums.net

Assistant U.S. Attorney Hsu has handled Intellectual Property cases in Los Angeles for more than a decade. He knows the peer-to-peer sites well. "Peer-to-peer is incredibly unsafe. It's not designed to be safe. It's the opposite of safe. And if you are a hacker that's sort of interested in compromising people, I mean you will use any tool in your toolbox, and so one of the tools in the toolbox is sending the RAT over peer-to-peer."

On Hack Forums, we see experienced ratters with skills like Luis Mijangos share tips and tools via YouTube with script kiddies, the next generation of Jared James Abrahamses. When ratters are ready to push the malicious downloads onto an unsuspecting audience, both YouTube and the content theft sites provide a platform for launching Trojans. We found several conversations on Hack Forums where ratters suggest both YouTube and content theft sites as the tools of choice for RAT spreading.



Searching for a good met ×

www.hackforums.net[redacted]

Welcome to HackForums.net

Current time: 05-06-2015, 02:04 PM

Hack Forums
Packets, Punks, and Posts
Home Upgrade Search Members Extras Wiki Help Follow Contact

Welcome back, outhaul4dca. You last visited: Today, 12:07 PM (User CP — Log Out)
View New Posts | Your Threads | Your Posts | Private Messages (Unread 1, Total 1)

Open Buddy List

Hack Forums / Hacks, Exploits, and Various Discussions / Hacking Tools and Programs / Remote Administration Tools / Searching for a good method to spread RATs

Thread Rating: New Reply

Searching for a good method to spread RATs

Thread Options

05-01-2015, 11:17 AM

Post: #1

Pider2k3
[nobody@HF:]

Prestige: 0
Posts: 11
Joined: Dec 2014
Reputation: 0

Hi Boys,

i would love to hear about some methods how u spread your RATs.

I was using following methods till now:

- Sharing Cracked Software via Torrent
- Mass Chat Rooms
- Make Youtube Videos of Something and add your file.

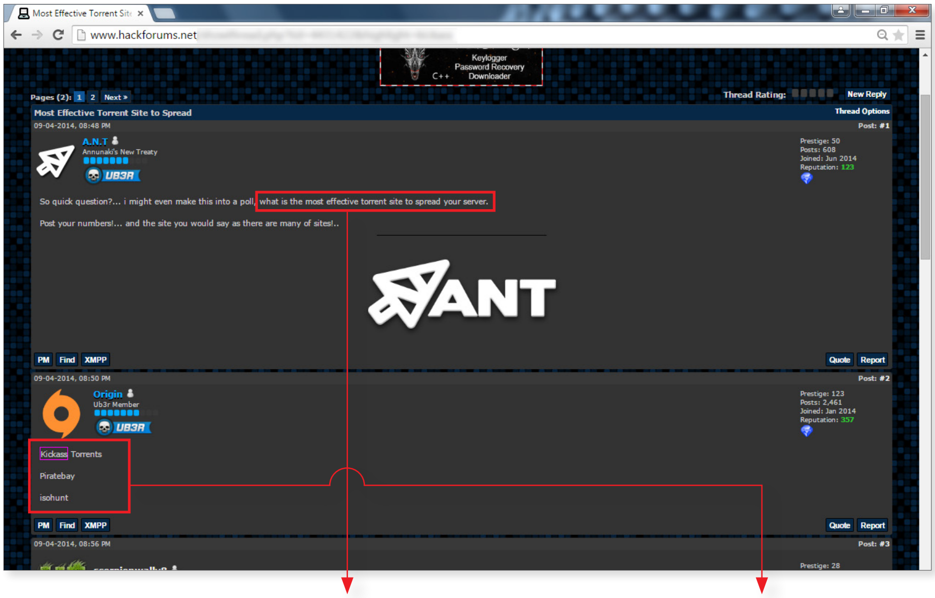
can someone tell me some other methods how u spread your rats? Would love to try some new methods, cause im bored of always the same...

Thank you.

- Sharing Cracked Software via Torrent
- Mass Chat Rooms
- Make Youtube Videos of Something and add your file.

IMAGE 26

• From the hackers' chat room, hackforums.net



Most Effective Torrent Site ×

www.hackforums.net[redacted]

Most Effective Torrent Site to Spread

09-04-2014, 08:48 PM

Post: #1

A.N.T
Annunaki's New Treaty

Prestige: 50
Posts: 608
Joined: Jun 2014
Reputation: 123

So quick question?... i might even make this into a poll, what is the most effective torrent site to spread your server.

Post your numbers!... and the site you would say as there are many of sites!..

09-04-2014, 08:50 PM

Post: #2

Origin
Ub3r Member

Prestige: 123
Posts: 2,461
Joined: Jan 2014
Reputation: 357

Kickass Torrents

Piratebay

isohunt

09-04-2014, 08:56 PM

Post: #3

Prestige: 28

what is the most effective torrent site to spread your server.

Kickass Torrents

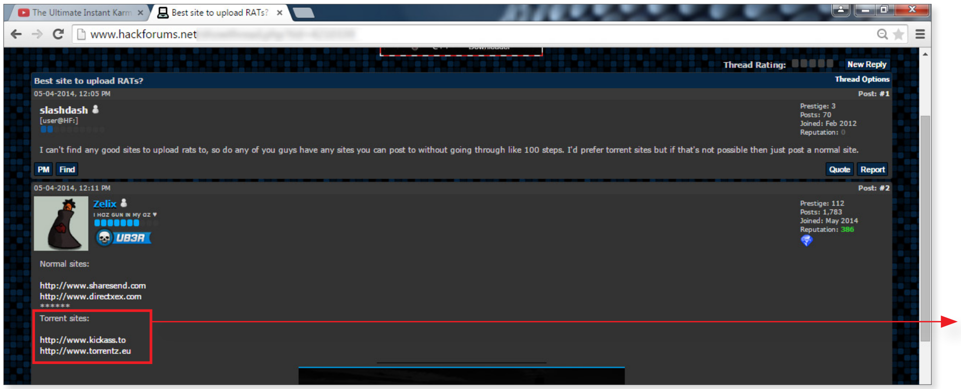
Piratebay

isohunt

IMAGE 27

• From the hackers' chat room, hackforums.net

When ratters wanted advice about specific content theft sites, it is no surprise that the names traded on Hack Forums are some of the most familiar to those who follow the piracy trade—kickasstorrents, isohunt, and The Pirate Bay (image 27, above).


The Ultimate Instant Karm
Best site to upload RATs?
www.hackforums.net[redacted]
Thread Rating:
New Reply
Thread Options
PM
Find
Quote
Report

Best site to upload RATs?

05-04-2014, 12:05 PM Post: #1

slashdash
[user@HF:]

Prestige: 3
Posts: 70
Joined: Feb 2012
Reputation: 0

I can't find any good sites to upload rats to, so do any of you guys have any sites you can post to without going through like 100 steps. I'd prefer torrent sites but if that's not possible then just post a normal site.

05-04-2014, 12:11 PM Post: #2

Zelix
I HOZ GUN IN MY OZ ♥
UB3R

Prestige: 112
Posts: 1,783
Joined: May 2014
Reputation: 386

Normal sites:

http://www.sharesend.com
http://www.directxex.com
******
Torrent sites:

http://www.kickass.to
http://www.torrentz.eu

IMAGE 28

• From the hackers' chat room, hackforums.net

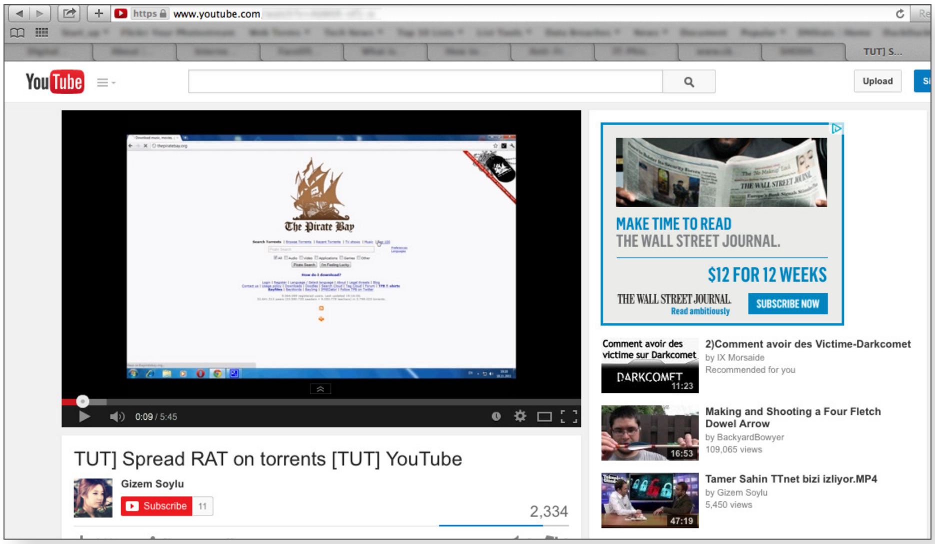
Torrent sites:

http://www.kickass.to
http://www.torrentz.eu

Some ratters go beyond just chatting about content theft sites; they show script kiddies how to use them—again in tutorial videos shared on YouTube. We found examples—again with advertising alongside the videos—of YouTube videos walking viewers through how to build deceptive, RAT infested traps to ensnare victims.

For example, one YouTube video (which we found posted by two different people) demonstrated how a ratter pulled an application from The Pirate Bay[f] to help spread a RAT. At one time, The Pirate Bay was the 97th most visited site in the world[15] and had more than 2 million registered users.[16] We watched the ratter take what looks like a clean application—in this case, a music editing application—from Pirate Bay, and corrupt it.

Moments later, the ratter loaded the corrupted file onto another popular torrent site, Demonoid.me. According to the Google Transparency Report (on 7/6/15), copyright holders have asked for more than 190,000 URLs to be taken down from Demonoid.me in the last six months, but that's just the beginning of the problems with this site. Demonoid.com was so infested with malicious downloads that



TUT] Spread RAT on torrents [TUT] YouTube
Gizem Soylu
2,334

2)Comment avoir des Victime-Darkcomet
by IX Morsaide
Recommended for you

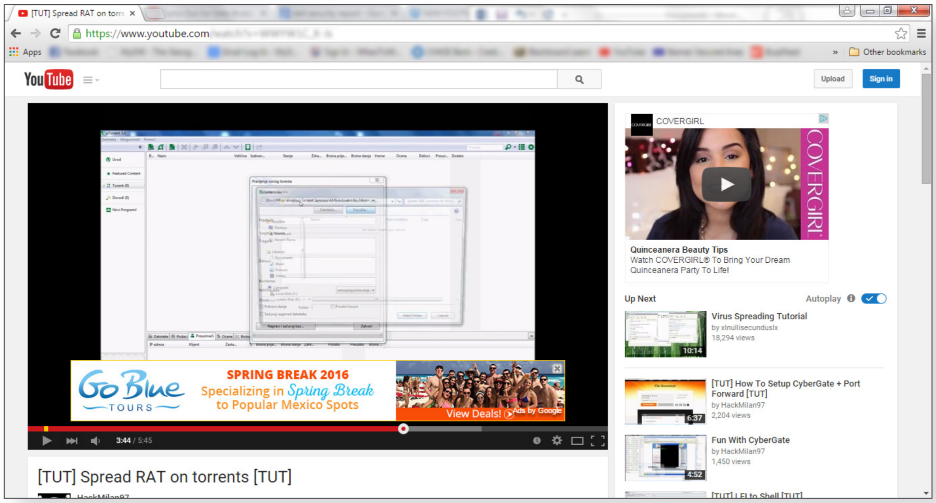
Making and Shooting a Four Fletch Dowel Arrow
by BackyardBowyer
109,065 views

Tamer Sahin TTnet bizi izliyor.MP4
by Gizem Soylu
5,450 views

IMAGE 29

• At the time of this screenshot, this video had 2,334 views.

[f] The video showed the ratter using piratebay.org. According to Wikipedia, piratebay.org was the address of the Pirate Bay until 2012, when it moved to piratebay.se. It has also used piratebay.gl. From http://en.wikipedia.org/wiki/ The_Pirate_Bay#cite_note-domainse-180 and https:// thepiratebay.se/blog/205.



Quinceanera Beauty Tips
Watch COVERGIRL® To Bring Your Dream Quinceanera Party To Life!

Up Next — Autoplay

Virus Spreading Tutorial
by xlnullisecunduslx
18,294 views
10:14

[TUT] How To Setup CyberGate + Port Forward [TUT]
by HackMilan97
2,204 views
6:37

Fun With CyberGate
by HackMilan97
1,450 views
4:52

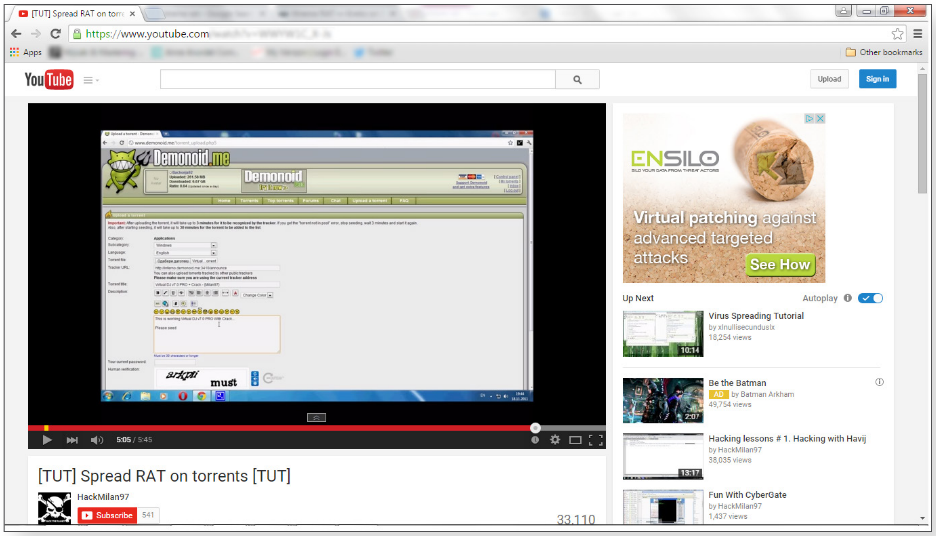
[TUT] LFI to Shell [TUT]

[TUT] Spread RAT on torrents [TUT]

HackMilan97

IMAGE 30

- At the time of this screenshot, this video had 13,643 views.



[TUT] Spread RAT on torre ×
https://www.youtube.com
Apps
Other bookmarks
YouTube
Upload
Sign in
Demonoid.me
Demonoid
ENSILO
SILO YOUR DATA FROM THREAT ACTORS
Virtual patching against advanced targeted attacks
See How
5:05 / 5:45

Up Next — Autoplay

Virus Spreading Tutorial
by xlnullisecunduslx
18,254 views
10:14

Be the Batman
AD by Batman Arkham
49,754 views
2:07

Hacking lessons # 1. Hacking with Havij
by HackMilan97
38,035 views
13:17

Fun With CyberGate
by HackMilan97
1,437 views

[TUT] Spread RAT on torrents [TUT]

HackMilan97
Subscribe 541
33,110

IMAGE 31

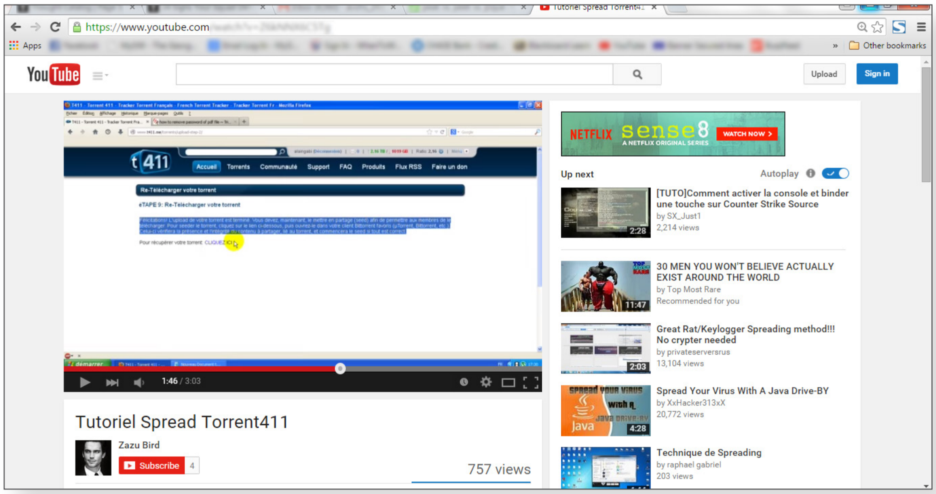
- At the time of this screenshot, this video had 33,110 views.

Google actually blocked it for a time in 2014.[17] But Demonoid has had more lives than a cat. The site stays alive by utilizing several Top Level Domains, including .com, .me, .ph, and it's current home at .pw (the others now redirect there). Alexa ranks the site as the 7,581st most popular site in the world (as of 7/6/15). Demonoid blamed the malicious downloads on advertising.[18] The Digital Citizens Alliance report, *Good Money Still Going Bad*, showed that one of every three ads on 589 content theft sites studied in that research had the potential to infect users' devices. The research also showed that content theft sites make money when users click on and download the malicious software from that advertising.[19]

In another YouTube video, we found a ratter demonstrating how to disguise a malicious payload as a PDF file using the content theft site T411.me[g]. The presenter also reminds the watcher to make the presentation nice so they can get more money from the victims.

In a third tutorial, a ratter shows how to use the RAT CyberGate. He pulls three addresses (saying in the tutorial that he has "only three vic's online") and then pulls the most popular software from three "torrent sites": demonoid.com. isohunt.com, and btjunkie.org, then reloads those sites with the now infected software.

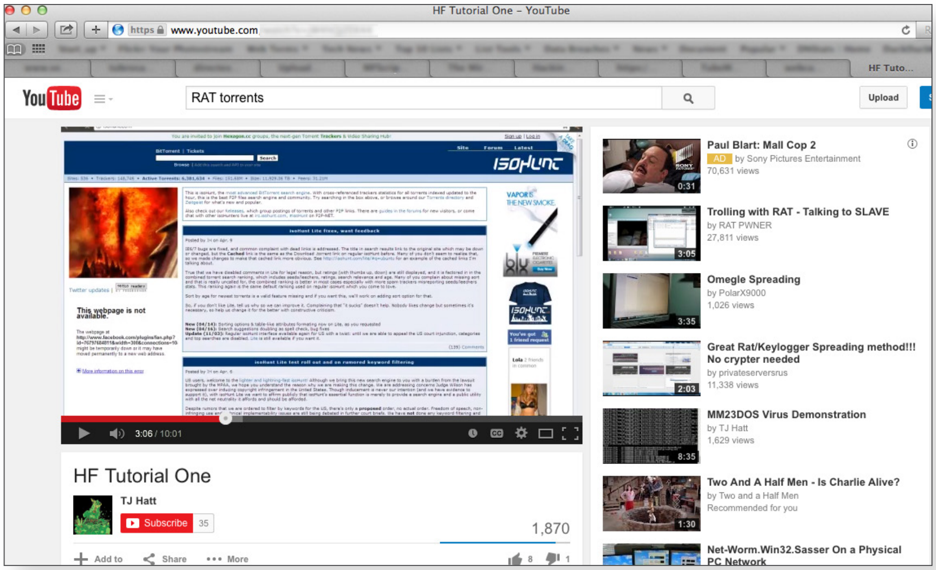
The tutorial videos show that for the ratters looking for the tools to spread their malware, content theft sites are like Home Depot.



https://www.youtube.com
YouTube
Upload
Sign in
t411
NETFLIX sense8 A NETFLIX ORIGINAL SERIES WATCH NOW
Up next
Autoplay
[TUTO]Comment activer la console et binder une touche sur Counter Strike Source
30 MEN YOU WON'T BELIEVE ACTUALLY EXIST AROUND THE WORLD
Great Rat/Keylogger Spreading method!!! No crypter needed
Spread Your Virus With A Java Drive-BY
Technique de Spreading
1:46 / 3:03
Tutoriel Spread Torrent411
Zazu Bird
Subscribe
757 views

IMAGE 32

• A video showing how to spread a RAT via the content theft site, t411.me. To the right of the video is an ad for the licensed and legal content provider of on-demand Internet streaming media, Netflix.



HF Tutorial One - YouTube
www.youtube.com
YouTube
RAT torrents
Upload
isoHunt
Paul Blart: Mall Cop 2
Trolling with RAT - Talking to SLAVE
Omegle Spreading
Great Rat/Keylogger Spreading method!!! No crypter needed
MM23DOS Virus Demonstration
Two And A Half Men - Is Charlie Alive?
Net-Worm.Win32.Sasser On a Physical PC Network
3:06 / 10:01
HF Tutorial One
TJ Hatt
Subscribe
1,870

IMAGE 33

• Isohunt was one of three sites known to be unlicensed content providers featured in this video.

[g] t411.me is one of 5—sites found to be sharing torrents unlicensed movies, TV series, music, books, software, and sports in Digital Citizens' *Good Money Still Going Bad* report published in May 2015. That domain now redirects to t411.io.

THE FUTURE OF RATS

This is where it gets really scary.

As with many other industries, once a new idea or process comes to the market place, it will filter down to all competitors in that space. This same trickle-down effect will happen to RATs according to Kevin Haley, one of the technical advisors on Symatec's *Internet Security Threat Report (ISTR)* and the Director of Product Management for Symantec Security Response. Haley told Digital Citizens: "I think we are going to see a lot of these things that are showing up in these high-end RATs work their way down into the low end. So the next thing we may be talking about is some stealth capability in Dark Comet which was in Regin [and] somebody figured out how to add it to that."

Stealth capabilities, or the RAT's ability to stay hidden, made it possible for Carbanak to stay cloaked for years, and therefore for the hackers to gather enough information to steal approximately $1B.[20] Bringing this attribute to script kiddie RATs will be a new burden on users. It's one of three traits that Haley says will be prominent in the next generation of RATs. The others:

Modularity—This means the RAT has the ability to add new functionality. If a basic RAT comes with system management (looking at files, operating the camera, etc.), you can get add-ons that allow the RAT to launch DDoS attacks, mine bitcoins, or have dropper or downloading capabilities. This is similar to getting the base model of a car and adding options such as leather seats, upgraded stereo, etc.

Customization—Taking a RAT and modifying it to have one core function. The Dyre RAT is a banking focused RAT—not so much on individual account holders, but more at the institutional level. Malware that mines bitcoins or attacks industrial control systems, like Havex[21], are examples of customized RATs.

"There's actually some movement to software as a service as a way to try and prevent [theft of source code] from happening." Haley says. Hackers are tired of their code getting stolen and distributed with no revenue coming to the original source. Having a cloud based service where any person can go use these tools to get a customized RAT without being able to pirate it is a concept that is not far off. This means in the future you can take the best qualities of all RATs and customize it for the attack you want to execute.

A "growth market" for ratters is mobile. A new generation of RATs tailored to strike cell phones and tablets, or mobile Remote Access Trojans (mRAT) is coming. As people move more towards having their wallet in their smartphone, the more these devices will be targeted. Ethical hacker Georgia Weidman, who writes about mobile hacking in her book "Penetration Testing, A Hands-On Introduction to Hacking" said "Though most people have their laptop in their bedroom these days, there is literally nowhere our phones, tablets, smart watches, etc. don't go. As they go from home, to work, to school, to the coffee shop, to your business trip to China, they likely encounter lots of different mobile and wireless networks with malicious actors."

You can see in image 34 the RAT Adwind has been modified to include not just desktop OS, but also mobile OS like Android.

What's particularly stunning is how fast it's growing. Using figures from the AV-Test Malware Repository, the anti-virus maker TrendMicro figured that while it took 22 years to get to 2 million distinct malware signatures for PCs, it has taken less than ten years to reach the same number with mobile devices.[22]

This growth, although alarming, is not surprising since smartphones are ubiquitous throughout the world. The bigger the distribution, the better it is for the hackers and criminals who continually target them. Weidman further states "And if you thought your laptop knew a lot about you think about everything your phone knows, calls, text messages, emails, geolocation, the list goes on."

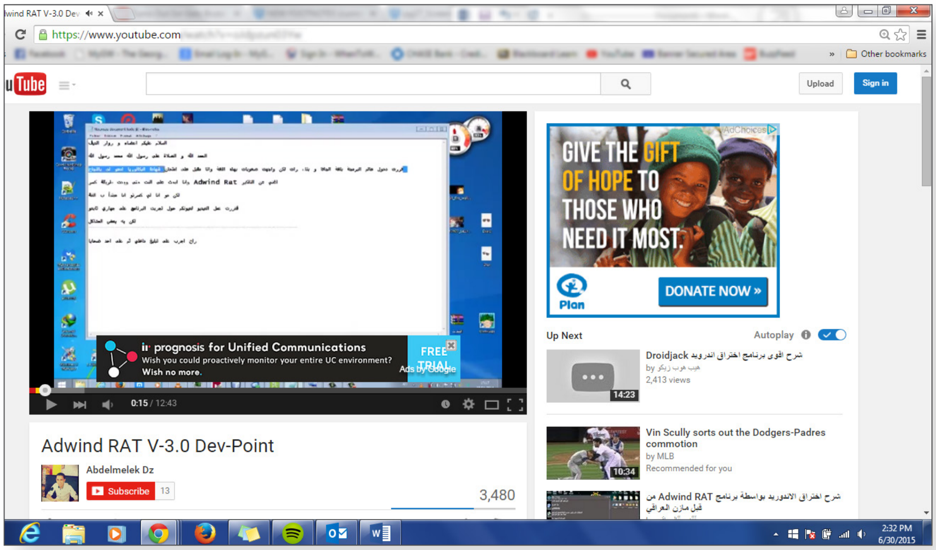

https://www.youtube.com
YouTube
Upload
Sign in
GIVE THE GIFT OF HOPE TO THOSE WHO NEED IT MOST.
Plan
DONATE NOW »
Up Next
Autoplay
Droidjack
14:23
2,413 views
Vin Scully sorts out the Dodgers-Padres commotion
by MLB
Recommended for you
10:34
Adwind RAT
prognosis for Unified Communications
Wish you could proactively monitor your entire UC environment? Wish no more.
FREE TRIAL
Ads by Google
0:15 / 12:43
Adwind RAT V-3.0 Dev-Point
Abdelmelek Dz
Subscribe
13
3,480
2:32 PM
6/30/2015

IMAGE 34

• At the time of this screenshot, this video had 3,480 views.

PROTECTING FROM AND REMOVING RATs

Digital Citizens' researchers have put together an extensive checklist that you can use to help protect yourself. Ultimately, we all have to understand that there isn't one thing that we can do to protect ourselves from ratters, but these steps give you a better chance at avoiding a RAT attack.

Protecting your system and the data it contains should be the same priority as protecting your wallet and passport. There are some basic things you should do to protect your system.

1. Create and use a secure password. Using a passphrase is even better. Check out http://www.cox.com/residential/support/internet/article.cox?articleId=232f2e00-ce8d-11e0-52e6-000000000000 for some ideas how to do it.
2. Never operate your computer using the first or Admin account. Create a second user with a different password so if you do something stupid, installing the RAT will ask you for your password. And that password prompt should make you realize you probably don't need to enter a password to listen to a song or watch a movie.
3. Only connect to your mail server using an encrypted connection. This prevents your password from being sent unencrypted, which allows attackers very easy access for bypassing basic security.
4. Being aware of where you connect has nothing to do with security. It's very easy to operate a computer from Starbucks; it's also easy enough to encrypt your network activities while you are at Starbucks.

This whole thing can be summed up in a simple word—educate yourself on how to safely use computers, and always assume the worst. Don't blindly click on pop up errors without reading them first.

→ Patch your OS and web browsers regularly and install applications updates as they are released. Manufacturers update their applications once vulnerabilities are found. This will not stop new viruses, but will protect against known viruses.

→ Have an Anti-Virus ("AV")[h] program installed and keep it up to date. There are many AV programs on the market and some are free. Look at AV ratings at http://www.pcmag.com/reviews/anti-virus. This goes for your smartphone too, especially if you do a lot of transactions on your phone.

→ Be aware of where you connect to the Internet. Connecting your system at coffee shops and other locations with free Wi-Fi means others can possibly monitor what you are doing and even capture passwords and other information.

→ Emails from unknown users should be treated with caution. Even emails from known users, which seem out of character for that individual, should be screened. Malware, including Trojan viruses, are linked to phishing attacks. According to SpywareRemove.com, an anti-virus organization, "Poison Ivy backdoor attacks have been linked to spam email messages that pretend to be sent by the webmaster of a career database website."[23] Hackers count on you being curious or too busy to realize what you are doing by clicking on a link within an email.

[h] Webroot defines Anti-virus software as "a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, (T)rojans, adware, and more." http://www.webroot.com/us/en/home/resources/tips/pc-security/security-what-is-anti-virus-software

→ When surfing the Internet, be alert for potential dangers. In a posting on Yahoo which address how to remove Trojan viruses like Poison Ivy, one participant noted "but it's a general consensus that this Trojan normally infects through hacked movie files. If you've been downloading movies from the Internet, you may want to consider using virus protection from now on."[24] A recent DCA report shows the correlation between movie and torrent files and malware.

There are many companies that make anti-virus applications. Also, many of these make specific supplemental program for removing viruses like Poison Ivy.

If you suspect you are infected, then do the following:

→ Cover your camera with an opaque piece of paper to avoid being spied on

→ Get one or more of the applications or steps in the reference section to remove the Trojan. Go to a clean system to do the research and download the application.

» NOTE: using two different applications from different companies will confirm that the Trojan is eliminated. Make sure the applications you use are up to date otherwise it will not get the latest version of the Trojan.

→ Do not do any more transactions or posts until you are sure the system is free from the virus.

» The safest thing to do is not to use the system for anything besides cleaning it until you are sure the system is virus free.

Once your system is free of the Trojan, do the following:

→ Change your passwords. If you have multiple passwords for multiple sites or application, you may need to utilize a password manager.

» If infected, any web password is most likely compromised. This is an annoying process, but important to mitigate residual effects of the infection.

→ Clear your web browser cache and history.

→ Patch the Operating System and the web browsers.

→ Do a system back-up and set a new restore point.

→ When in doubt, take your system to a trusted organization that can remove the Trojan for you.

MORE REFERENCES ON RAT REMOVAL

→ http://www.ehow.com/how_6815580_remove-poison-ivy-trojan.html

» Tips on removing Poison Ivy Trojan

→ https://answers.yahoo.com/question/index?qid=20080916214402AAsP2UQ

» This has links to several AV apps (Trend Micro, McAfee, Symantec)

→ https://security.symantec.com/nbrt/overview.aspx?

» Symantec tools

→ http://www.spywareremove.com/removePoisonIvy.html

» Has tool associated with it

→ http://winzip.com/prodpagemp.html

» Winzip Product

→ http://www.clamav.net/index.html

» This tool is a one-time scanner type AV—not continuous protection. Good to identify and remove a Trojan, but does not continuously scan your system.

→ http://www.pcmag.com/reviews/antivirus

» Review of anti-virus programs

SUMMARY AND RECOMMENDATIONS

There is no doubt that the most serious offenders here are the ratters themselves. When law enforcement identifies and prosecutes one, others sprout up to take over. For starters, prosecutors should be able to charge ratters who attack young women and girls with sex crimes. Forcing women to perform sexual acts on camera is sexual assault, pure and simple. Stronger sentences will almost certainly drive some script kiddies to hesitate before attacking women. Criminal activity should be treated equally whether it's on the street corner or in the darkest corners of the Internet. Consider the message from sentencing of former Silk Road kingpin Ross Ulbricht, who was sentenced to life in prison. The deaths of the people who bought drugs on the Silk Road were not a digital experience, and now the person responsible for making those drugs available over the Internet was dealt real world justice.

But what about the enablers?

Quite simply, regular visits to content theft sites will infect your computer. The more research we do, the more we see traps and dangerous material on these sites. Operators of these sites claim to be providing a service, but some of them in fact make money by infecting your computer. MediaLink researchers working on our May 2015 report, *Good Money Still Going Bad*, found many malicious ads are pay-per-click ads. That means the site's operators don't make money until the user clicks the ad and downloads the malicious file. If you feel the value of free movies and music is worth the risk to your device, your personal information, and your well being, you might want to reconsider your priorities.

As for the videos on YouTube, this is a bit more complicated. This is the fifth Digital Citizens Alliance report looking at dangerous videos posted on YouTube which generate advertising revenues for Google. The previous four reports all looked at videos that marketed illegal activity. After media coverage of our research, YouTube pulled down hundreds of videos marketing appearance-and-performance-enhancing-drugs (steroids), stolen credit cards, illegal drugs, and prescription drugs available without a doctor's approval. While spreading a RAT is illegal, showing someone how to do it is, well, something of a grey area. As Assistant U.S. Attorney Hsu says "it depends on the content of the video and the intent of the person posting the video." There are plenty of videos that include ratters talking about getting victims, sharing public IP addresses, and featuring the faces of those whose devices they've slaved. On the other hand, white hats also view and share videos about Remote Access Trojans. Pulling all these videos down could harm ethical hackers' efforts to study malware.

But ethical hackers would not post videos that "invade" a person's home, showing pictures of victims and sharing public IPs. There's no reason for videos with those elements to find a home on YouTube.

However, there is nothing stopping YouTube from sharing RAT tutorials. But just because YouTube can, does it mean it should?

"Google used to pride itself on the statement 'don't be evil,'" said Scott Aken. "Well, in this case, for people that are putting videos out there where their videos are clearly directed towards evil, should you allow these people to make money off that? That's the question they need to ask themselves."

This could be a moment for Google much like that for CVS when the drug store chain stopped selling cigarettes in September 2014. The pharmacy's executives decided they could no longer justify how a company dedicated to keeping customers healthy could profit from a product producing profound health risks.

It is time for Google to stop running advertising next to videos showcasing ratters' purges of private personal moments and sensitive information. Slaving a device may not be a physical attack, but it could be just as devastating and painful to the victims of RAT attacks. No one—be it a ratter or a multibillion dollar company—should make one penny of profit from these attacks. There is no reason why a great company like Google and one of its products, YouTube, should be the ratters' tool of choice. Yet as we saw from numerous conversations on Hack Forums, YouTube provides a forum where the Mijangoses, the Abrahamses, and future super-ratters can spread their terror.

So could Google add some safeguards to its advertising partner programs, like AdSense?

Google might argue that the company has the solution to the problems it is creating. To its credit, Google has made efforts to keep child pornography off its platforms. Recently, the company announced an effort to protect revenge porn victims. But what about getting tough on tools used to make child porn, revenge porn, and violate the right to privacy of women and children around the world?

Google does on occasion use human beings to check items its automated systems may not always catch. In March, Google announced that an internal team looking for policy violations would review app submissions to Google Play.[25] In 2013, Google brought in 200 engineers to spot and block child pornography and blocked 100,000 search terms associated with child porn.[26] Why can't Google create a human team to review malware tutorials videos on YouTube looking for those that include pictures of victims and their IPs?

Scott Aken had a suggestion for Google: further develop their safe browsing technology within Chrome that could help detect more malicious links 'before' people click on them. "Google already has a lot of this data. What if they use some of their resources to further plow all of this data into a pool and if you are presented with a link to a malicious website, they could say, 'Sorry—you're not allowed to access that website because it's dangerous.'"

Such steps would cost Google money. But will Google take action to stem a rising tide of RATs spreading across devices all over America? Or, will they continue to put profits before people. We hope that the people at Google decide it is time to think about the future.

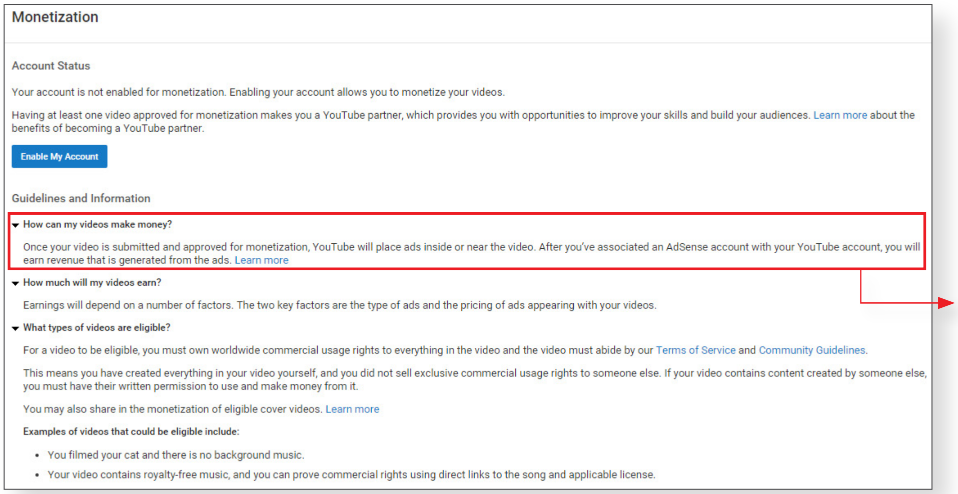
We're not asserting Google has committed a crime. As a consumer advocacy group, we believe the company can use its tools and skills to help ward off the ratters that are selling "slaving" in these YouTube videos and the slow the spreading of their evil activities. Google is in a position to help solve the "slaving" problem, instead of profiting from it.

ONE SIMPLE QUESTION: WHO APPROVED THIS?

All the screen shots in this report included advertising at the time our researchers found them. Many of the people posting the videos are part of YouTube's Partner Program. They have given YouTube permission to include the ad while, in return, YouTube agrees to give them a split of the advertising revenue.

In order to be a member of the YouTube Partner Program, the content creator must start a Google AdSense account to begin monetizing their content. The YouTube Partner Program's guidelines on monetization state that each video must be "approved for monetization" to enable advertising which, in turn, allows the "YouTube Partner" to receive a split of the revenues.

So someone, or something, "approved" the videos running with Partner Program advertising. Who, or what, would approve advertising next to videos that humiliate children? YouTube hasn't answered questions about how ads could run next to videos sympathetic to ISIS, even with many advertisers wondering how that could happen.[27] Right now, Google splits revenues 55/45 with eligible YouTube Partner Program participants. There is no



Monetization

Account Status

Your account is not enabled for monetization. Enabling your account allows you to monetize your videos.

Having at least one video approved for monetization makes you a YouTube partner, which provides you with opportunities to improve your skills and build your audiences. Learn more about the benefits of becoming a YouTube partner.

Guidelines and Information

▾ How can my videos make money?

Once your video is submitted and approved for monetization, YouTube will place ads inside or near the video. After you've associated an AdSense account with your YouTube account, you will earn revenue that is generated from the ads. Learn more

▾ How much will my videos earn?

Earnings will depend on a number of factors. The two key factors are the type of ads and the pricing of ads appearing with your videos.

▾ What types of videos are eligible?

For a video to be eligible, you must own worldwide commercial usage rights to everything in the video and the video must abide by our Terms of Service and Community Guidelines.

This means you have created everything in your video yourself, and you did not sell exclusive commercial usage rights to someone else. If your video contains content created by someone else, you must have their written permission to use and make money from it.

You may also share in the monetization of eligible cover videos. Learn more

Examples of videos that could be eligible include:

- You filmed your cat and there is no background music.
- Your video contains royalty-free music, and you can prove commercial rights using direct links to the song and applicable license.

IMAGE 35

• YouTube monetization guidelines and information found at https://www.youtube.com/account_monetization

• How can my video make money?

Once your video is submitted and approved for monetization, YouTube will place ads inside or near the video. After you've associated an AdSense account with your YouTube account, you earn revenue that is generated from the ads.

incentive for Google to end such a program—unless the company hears from the very advertisers who—unintentionally—make this revenue possible. It is the companies that see their ads running next to these videos marketing 'slaving' that could force Google to act; this would likely result in more aggressive monitoring and rejection of videos that put money in the pockets of the pushers of malicious materials.

Google and YouTube have fended off these questions for a while. In 2013, after two States Attorneys General questioned Google officials about profits from videos marketing illegal and illicit activities, The Oklahoman newspaper reported that Google "derives 'minimal' income from the questionable videos." To be clear—the word "minimal" was Google's own description from its response to the AGs' letter.[28] If it is so "minimal," then why does Google need to continue to run ads next everything from ISIS videos to illegal drugs to Remote Access Trojan tutorials?

If Google continues to sell ads beside slaving videos, can it claim Internet freedom as a defense? If one of the world's most admired companies takes a stand against slaving, others will follow.

Perhaps the best advice on how the company could handle that question came from Cassidy Wolf, who said she would tell Google: "They need to put themselves in (the victim's) shoes... and imagine if it was their daughter that was being watched in their room and now its being promoted on YouTube and the people that are doing this are making money of this and Google is making money off of this. Honestly, I would just tell them to put themselves in the victim's shoes and imagine if this was happening to them."

IF YOU SEE A VIDEO SHOWING VICTIMS OF RATTERS,
YOU CAN REPORT THE VIDEO TO YOUTUBE AT
https://support.google.com/youtube/answer/2802027?hl=en.

APPENDIX A

Companies/Products for which Digital Citizens researchers found advertisements on pages with RAT promotional videos on YouTube in the fourth quarter of 2014 and first half of 2015.

Acura (pg. 17, Image 14)—found November 14, 2014
Allstate Boat (pg. 14, Image 8)—found April 12, 2015
American Express Travel (pg. 7, Image 2)—found February 25, 2015
Audible, an Amazon Company (pg. 8, Image 3)—found April 10, 2015
Batman Arkham Knight (pg. 7, Image 2)—found February 25, 2015
Boeing (pg. 21, Image 21)—found March 17, 2015
Chevrolet (pg. 3, Image 1)—found December 4, 2014
CoverGirl (pg. 27, Image 30)—found June 30, 2015
Ensilo (pg. 27, Image 31)—found June 22, 2015
ESPN Fantasy Football (pg. 19, Image 15)—found July 7, 2015
Geico (pg. 13, Image 7)—found April 29, 2015
Go Blue Tours, (pg. 27, Image 30)—found June 30, 2015
Mini Cooper (pg. 20, Image 17)—found June 25, 2015
Netflix (pg. 28, Image 32)—found July 16, 2015
New York Yankees Ticket Exchange (pg. 20, Image 18)—found March 3, 2015
Plan (pg. 30, Image 34)—found June 30, 2015
Procter & Gamble

- » Bounty (pg. 13, Image 6) (featuring characters from NBCUniversal film *Minions*)—found July 7, 2015
- » Always (pg. 21, Image 22)—found July 8, 2015

Samsung (pg. 21, Image 20)—found December 3, 2014
Starbucks / Arizona State University (pg. 16, Image 12)—found April 12, 2015
Sony Pictures Entertainment, *Paul Blart, Mall Cop 2* (pg. 28, Image 33)—found April 14, 2015
The Wall Street Journal (pg. 26, Image 29)—found April 25, 2015
Unified Communications (pg. 30, Image 34)—found June 30, 2015
Vans Off the Wall (pg. 8, Image 3)—found April 10, 2015
Wells Fargo (pg. 19, Image 16)—found July 16, 2015
Zulily (pg. 20, Image 19)—found July 17, 2015

EACH SCREENSHOT OF YOUTUBE PAGES AND WEBSITES WAS GRABBED DURING DIGITAL CITIZENS RESEARCH AND MAY NOT REFLECT THE CURRENT STATUS OF ANY PAGE.

APPENDIX B

Slaved Devices Found From Information on YouTube

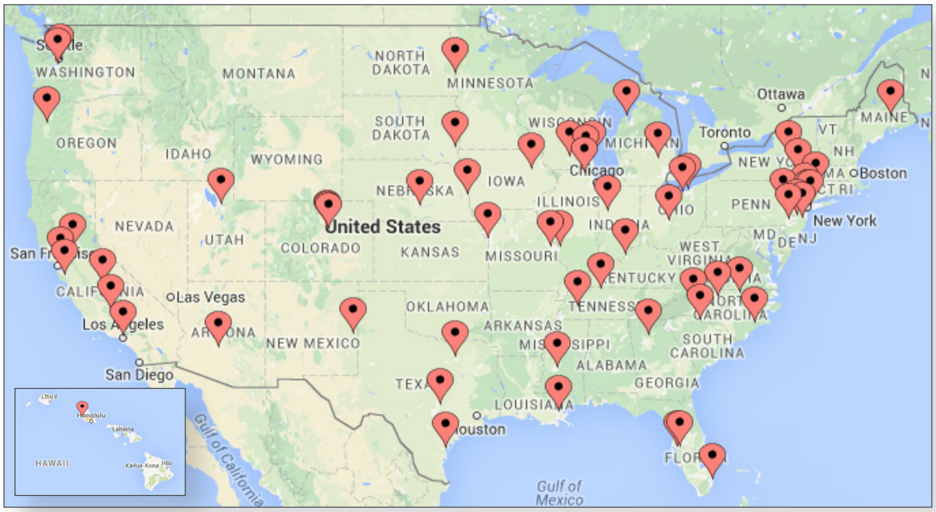


IMAGE 36

• The map includes IP addresses in videos with and without ads.

IPs in these cities found on Videos with Ads:

Albany, OR
Alpharetta, GA
Bakersfield, CA
Brandon, FL
Chesterfield, MO
Clarksville, TN
Collinsville, IL
Columbus, OH
Corpus Christi, TX
Denver, CO

Fargo, ND
Greensboro, NC
Highlands Ranch, CO
Jackson, MS
Jackson, NJ
Jackson, TN
Kansas City, KS
Kearney, NE
Los Angeles, CA
Los Gatos, CA

Louisville, KY
Milwaukee, WI
Mukwonago, WI
New York, NY
Omaha, NE
Phoenix, AZ
Ramsey, NJ
Sacramento, CA
Sanger, CA
Sherman, CT

Sioux Falls, SD
Tacoma, WA
Tampa, FL
Trenton, NJ
Tukwila, WA
Wai'anae, HI
Woodstock, IL

IPs in these cities found on Videos without Ads:

Austin, TX
Bala Cynwyd, PA
Catawba, SC
Cleveland, OH
Columbus, OH
Elyria, OH
Emeryville, CA

Flint, MI
Halcottsville, NY
Henderson, NC
Hickory, NC
Hollywood, FL
Independence, IA
Jacksonville, NC

Littleton, CO
Madison, WI
New Orleans, LA
New York, NY
Old Town, ME
Palmerton, PA
Phoenix, AZ

Portales, NM
Richardson, TX
Salt Lake City, UT
South Richmond Hill, NY
Suttons Bay, MI
Utica, NY
West Lafayette, IN

APPENDIX C

RAT Videos Running with Ads on YouTube:

SEARCH TERM	# OF RESULTS	VALID HITS (2 PAGES)	VALID HITS W/ADS	VALID HITS (%)	VALID HITS W/ADS (%)
How to download and use Poison Ivy RAT	2,500	28 of 34	9 of 34	82%	26%
How to download and use DarkComet RAT	9,920	40 of 40	19 of 40	100%	48%
How to download and use njRAT	11,300	40 of 40	19 of 40	100%	48%
How to download and use Blackshades RAT	2,250	38 of 40	14 of 40	95%	35%
How to download and use Bifrost RAT	4,520	33 of 34	10 of 33	97%	30%
TOTAL	**30,490**	**179 of 188**	**71 of 188**	**95%**	**38%**

The table above was compiled by using the following step by step approach:

1. Search for "How to download and use _ RAT"
2. Determine the number of results that come up for that search term.
3. Manually view each video on pages 1 and 2 of search results to determine the number of valid hits (for the criteria used to determine a valid hit read below).
4. Again manually view each video on pages 1 and 2 of search results to determine the number of valid hits with ads. A valid hit with ads had to meet the criteria for a valid hit and have at least one advertisement running next to or inside of the video.

Each video had to meet one or more of the following criteria to be determined a "valid hit":

1. Include the language, "How to use and download X RAT" in the title or the video itself.
2. Include a link to download the Remote Access Trojan specified in the video.
3. Include specific instructions during the video on how to download, spread, and/or use the Remote Access Trojan in the subject line.
4. Include a link to download a "crypter" that enables a Remote Access Trojan to go undetected on a victim's computer.
5. Include specific instructions during the video on how to download and/or use the "crypter" in the subject line.

According to Way 2 Hackintost, A Crypter is defined as software used to hide viruses, keyloggers or any RAT tool from anti-viruses so that they are not detected and deleted by anti-viruses.

For more go to:
http://way2h.blogspot.com/2013/02/what-is-crypter-how-it-works.html

ACKNOWLEDGEMENTS

For all the sad and cruel things that we saw while doing this research, we also learned of and saw many 1:1 acts of kindness. We are grateful to Cassidy and Mary Wolf for working with us. They provided our team with inspiration as we brought this story to light. Cassidy Wolf responds to RAT victims who reach out to her via social media looking for help and advice.

Hemanshu Nigam of SSP Blue has been fighting for the victims of hackers since before the Digital Citizens Alliance even existed. We thank him for educating us on this issue. We would not have had the previously mentioned conversation with the college student at Black Hat if "Hemu" hadn't suggested that we ask.

Also, we want to thank the cyber security analysts and experts for sharing their research and expertise. The cyber security community is on the front line of this fight to protect consumers.

Specifically, we'd like to thank these organizations for sharing their research publicly and answering our questions:

- Blackfin Security
- Dell SecureWorks
- Nielsen
- Symantec
- Verizon Enterprise Solutions

These individuals shared their expertise to helping understand some complicated issues:

- Scott Aken
- Gary Miliefsky, Snoopwall.com
- Will O'Neal, Mid-Atlantic Computer Solutions
- James Pastore
- Adam Rouse, Chicago-Kent College of Law Legal Fellow
- Georgia Weidman, founder of Bulb Security and Shevirah

Also, the law enforcement officials who discussed their work to protect consumers from dangerous individuals pushing malware:

- Wesley Hsu, Chief of the Cyber and Intellectual Property Crimes Section, U.S. Attorney's Office for the Central District of California
- Laura Eimiller, Press & Public Relations at U.S. Department of Justice (FBI)

There were some long hours spent on research for this report. We greatly appreciate those who helped us dig a little deeper in the search for answers:

- Meghan Green, President of the Cyberlaw Students Association, George Washington University Law School
- Patrick Osborne, Outhaul Consulting, LLC
- Lauren D. Shinn

Also, when we needed to produce this report, we got help from talented professionals who shared special skills:

- FoxDog Studio
- Greg Nelsen Photography
- TransPerfect

ENDNOTES

1 “What’s a Blackhat Hacker?” PC Tools. (http://www.pctools.com/security-news/blackhat-hacker/)

2 Gary Miliefsky, “2015: The Year of the Rat—Threat Report” (2015), *available at* http://www.snoopwall.com/wp-content/uploads/2014/12/2015-Year-of-The-Rat-by-Gary-SMiliefsky-SnoopWall_downloadPDF.pdf

3 Brian Krebs, “‘Blackshades’ Trojan Users Had It Coming” Krebs on Security (May 19 2014), http://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/

4 Dell SecureWorks, “Underground Hacker Markets,” (December 2014), *available at*, http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf

5 Criminal Complaint at 7, *U.S. v. Abrahams*, No. 8:13-cr-00199-JVS (C.D. Cal. Sept. 17, 2013)

6 Sasha Goldstein. “Calif. teen, guilty in Miss Teen USA ‘sextortion’ plot, sentenced to 18 months in prison” New York Daily News. 17 Mar. 2014. (http://www.nydailynews.com/news/crime/mastermind-teen-usa-sextortion-plot-18-months-prison-article-1.1724809)

7 Elizabeth Hagen & Rich Calder, “Over 90 Arrested in Cyber Breach that Ensnared Miss Teen USA,” *New York Post* (May 19 2014), http://nypost.com/2014/05/19/miss-teen-usahacked-again-in-massive-cyber-breach/

8 Nate Anderson, “Meet the Men Who Spy on Women Through Their Webcams” Ars Technica, (Mar. 10, 2013), http://arstechnica.com/tech-policy/2013/03/rat-breeders-meetthe-men-who-spy-on-women-through-their-webcams/

9 Based on figures from Nielsen

10 *Verizon 2015 Data Breach Investigations Report*, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015-insider_en_xg.pdf

11 Nate Anderson, “How an omniscient Internet “sextortionist” ruined the lives of teen girls” Ars Technica. 7 Sept 2011. (http://arstechnica.com/tech-policy/2011/09/07/how-an-omniscient-internet-sextortionist-ruined-lives/)

12 Robert McMillan, “Man gets 6 years for hacking victims’ computers to extort photos” ComputerWorld. 1 Sept 2011. (http://www.computerworld.com/article/2510927/cybercrime-hacking/man-gets-6-years-for-hacking-victims--computers-to-extort-photos.html)

13 Nate Anderson, “How an omniscient Internet “sextortionist” ruined the lives of teen girls” Ars Technica. 7 Sept 2011. (http://arstechnica.com/tech-policy/2011/09/07/how-an-omniscient-internet-sextortionist-ruined-lives/)

14 Lori Andrews, Michael Holloway, & Dan Massoglia, *Digital Peepholes Remote Activation of Webcams: Technology, Law, and Policy*. 2015. (http://www.ckprivacy.org/uploads/4/1/8/3/41830523/digital_peepholes_2015.pdf)

15 Bogdan Popa, “The Pirate Bay Joins Google and Yahoo in the Most Popular Websites Ranking” Softpedia. 19 May 2008. (http://archive.news.softpedia.com/news/The-Pirate-Bay-Joins-Google-and-Yahoo-in-the-Most-Popular-Websites-Ranking-85905.shtml)

16 “THEPIRATEPARTYBAY: THEPIRATEBAY.ORG AND THE PIRATEBAY.SE” TorrentFreak. (https://torrentfreak.com/the-pirate-bay/)

17 Andy, “Google Blocks Demonoid For Spreading Malicious Software” TorrentFreak. 8 May 2014. (https://torrentfreak.com/google-blocks-demonoid-for-spreading-malicious-software-140508/

18 Sasha Goldstein “Calif. teen, guilty in Miss Teen USA ‘sextortion’ plot, sentenced to 18 months in prison” *New York Daily News* (Mar. 17, 2014) http://www.nydailynews.com/news/crime/mastermind-teen-usa-sextortion-plot-18-months-prison-article-1.1724809

19 Digital Citizens Alliance, *Good Money Still Going Bad: Digital Thieves and The Hijacking of The Online Ad Business*. May 2015. (https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/298a8ec6-ceb0-4543-bb0a-edc80b63f511.pdf)

20 Limor Kessem, “Carbanak: How Would You Have Stopped a $1 Billion APT Attack?” Security Intelligence. 23 Feb 2015. (http://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/#.VZGQW_lVikr)

21 John Leyden, “Attackers fling Stuxnet-style RATs at critical control software in EUROPE” The Register. 26 Jun 2014. (http://www.theregister.co.uk/2014/06/26/industrial_control_trojan/)

22 “The Mobile Landscape Roundup: 1H 2014” Trend Micro. (Aug. 26, 2014), http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/the-mobile-landscape-roundup-1h-2014

23 SpywareRemove, “PoisonIvy” Spyware Remove. (Apr. 17, 2009), http://www.spywareremove.com/removePoisonIvy.html

24 Yahoo! Answers, “How do I remove the Poison Ivy virus from my laptop?” *available at* https://answers.yahoo.com/question/index?qid=20080916214402AAsP2 (last visited July 16, 2015)

25 Sarah Perez, “App Submissions On Google Play Now Reviewed By Staff, Will Include Age-Based Ratings” *TechCrunch*. (Mar. 17, 2015), http://techcrunch.com/2015/03/17/app-submissions-on-google-play-nowreviewed-by-staff-will-include-age-based-ratings/

26 Paul Resnikoff, “Google Is Now Blocking 100,000 Search Queries Related to Child Pornography...” Digital Music News (Nov. 18, 2013), http://www.digitalmusicnews.com/permalink/2013/11/18/googleblocking

27 Barrett J. Brunsman, “P&G seeks to halt ads from appearing with ISIS propaganda videos” Cincinnati Business Courier. 4 Mar 2015. (http://www.bizjournals.com/cincinnati/news/2015/03/04/p-g-seeks-to-halt-ads-from-appearing-with-isis.html)

28 Andrew Knittle, “Google claims it makes little money from videos with illegal or objectionable content” The Oklahoman. 18 Aug 2013. (http://newsok.com/google-claims-it-makes-little-money-from-videos-with-illegal-or-objectionable-content/article/3873056)

digital citizens
alliance