sumit 2013

nate anderson
THE
INTERNET
POLICE

HOW CRIME WENT ONLINE,
AND THE COPS FOLLOWED

NATE ANDERSON

"EXCELLENT." —CORY DOCTOROW, BOING BOING
DIRTY rats

adventures in the online underworld
BUT I HAVE TO COVER THE WEBCAM

OR THE HACKERS WILL SEE ME
LAPTOP HAS BUILT-IN WEBCAM

IMMEDIATELY TAPE PAPER OVER THE LENS
The Guys Spying On You Through Your Webcam
The Guys Spying On You Through Your Webcam
The hackers
"Recently I infected a person at my school with darkcomet. It was total luck that I got her infected because I suck at social engineering. Anyway, this girl happens to be a model and a really good looking one at that :D. I was hoping I could use her and her facebook account to further spread my darkcomet rat. I want to mass message all her friends on facebook but I have no idea what to message them to get them to download the rat. Any ideas or suggestions would be greatly appreciated :)."

"cutefuzzypuppy"
DARkcomet
DARKCOMET

credit: Malwarebytes
Darkcomet

credit: Malwarebytes
Darkcomet

credit: Malwarebytes
Just a “Prank”
I'm pretty sure that disabling the LED is hardware meaning if you turn on the webcam the LED will come on unless you take apart your webcam/laptop.

Cammy is old and outdated. I would recommend sticking with dc.

Here is a reference that will hopefully help you out. Credit goes to TheKey for this list.

**1.3M WebCam** = Safe to fully use, no light, no popup software.

**1.3M HD WebCam** = Light goes on, but mostly unnoticeable, no popup software.

**Integrated webcam** = Light goes on, bright as fuck, Dell Webcam Center goes up

**1.3M Integrated webcam** = Light goes on, bright as fuck, Dell Webcam Center goes up

**Sony blabla communication** (If it has Sony in it, you already know), bright fucking light, arcsoft pops up which takes long to hide in the window/minimize

**Video WebCam** = GOLDEN, no light, no software, 100% incognito

**Chicony USB 2.0 Camera** = Dimmed light, no software popup, good to use

**USB-Videodevice** = Good to use, might have a light on, no software popup

**USB 2.0 Camera** = No light, Arcsoft pops up/Might light up, lots of cheapshit/webcams use this driver

**USB UVC VGA WebCam** = No light/Light, Asus models have bright fucking light, is useable.

**Nagamura (or something like that) Camera** = Good to use, no light, no popup

**WebCam SCB-1900N** = Good to use, no light, no software
Luis Mijangos
Female victim was “visibly upset and shaking during parts of the interview and had to stop at points to control her emotions and stop herself from crying.” She did not leave her dorm room for a full week after the threats.

Affected her boyfriend, too; he later told a court that even his parents “had a hard time trusting anyone or even feeling comfortable enough to use a computer” after the episode.
Netbus

No connection
Netbus pro
Subseven
“ive had this girl since i started ratting but she has a light on her cam... shame coz shes really pretty with her hair down. see her busting me lol.”
"Using this method can easily get you around 500-3k installs a day and the methods are easy to
One poster said he had already archived 200GB of webcam material from his slaves. “Mostly I pick up the best bits (funny parts, the ‘good’ [sexual] stuff) and categorize them (name, address, passwords etc.), just for funsake,” he wrote. “For me I don't have the feeling of doing something perverted, it’s more or less a game, cat and mouse game, with all the bonuses included. The weirdest thing is, when I see the person you've been spying on in real life, I’ve had that a couple of times, it just makes me giggle, especially if it's someone with an uber-weird-nasty habit.”
The STATE (1): SCHOOLs
Lower merion
Lower Merion

In the wake of another theft incident in which six laptops were stolen from an HHS locker room in September 2008... Ms. Cafiero wrote that LANrev had captured images from one of the laptops; HHS Desktop Technician Amanda Wuest wrote, “This is awesome. It’s like a little LMSD soap opera,”
“Some teachers covered the lenses of the webcams on their laptops. Christine Jawork, a ninth grade teacher at HHS, advised us that she had told students that the District could remotely activate their laptops’ webcams as a means of tracking lost laptops, and that she had taped over the webcam on her laptop. She also said that her students had...
Window: "Sign In - Windows Internet Explorer"

swGOOD MORNING LOVE!!!GOOD Mo Backspace ORNING LOVE!!! Howes My DARLING Backspace Backspace Backspace w's Backspace Backspace Y Today???? I LOVE YOU BABY!!! MMMMMMMMMMMMWAAAAA!!!!! SUSAN'S BABY!!!!!!! Yaall! Enter Baby...I LOVE when I hear y Backspace Your "sweet" voic!!! Backspace Backspace Backspace Backspace Backspace e!!! When those "didgits" Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace phone...OH LORD!!! That's Backspace Backspace Backspace Backspace Backspace's what I'm talkin about!!! THRILL ME!!!! YES LORD!!! I Backspace "ABSOLUTILY Backspace Backspace Backspace Backspace BACKSPACE TELY Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace BACKSPACE L 'ADORE' MY MAN!!! I LOVE MY "SWEETNESS" AL Backspace Backspace Backspace Backspace!!! That would be YOU!!!! Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace YOU DARLIN!!! SUSAN' Backspace Backspace S PRECIOUS PEA!!!! Yaall! Giv aGimme Kiilissssssss!!!! MMMMMMMMMMMMMMMMMMMMMM MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM!!!! I Backspace Hope to see Your "cute" Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace sometime Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace time sooner than later!!! If only for a short time Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace period!! Duty calls!!! Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace Backspace BUT...I MISS YOU BABY!!!
The computer
Q. I see. You didn’t consider that it would potentially be an emotional trauma for this woman to be presented by you with photographs of her in sexually explicit positions that she had no intention that anybody else would see other than Mr. Smith?
A. No, sir.
Q. You didn’t think about it?
A. No, sir....
Q. You don’t think the very fact that you’re a police officer and you have the authority and you got a badge, you don’t think that’s intimidating to some people?
A. It could be.
Q. But you don’t think you’ve ever intimidated anybody?
A. I try not to. I may have, but that’s not my intention.
how susan saw it...

"I feel worthless. I cannot socialize like I used to, and in the past I was a very social person. I was in many clubs, professional. I could leave the house, I could shop for food. I could do things that now I cannot do... I can break out in a sweat when I see a police car. . . . My mind flashes back to the dehumanizing—what I call rape, when I can sit in the privacy of my own home and be spied on. It’s anxiety ridden... I never had to lock my bedroom door or put a lock and do all these things before or call [the] cable [TV company] every two minutes because I’m assuming somebody’s spying through my TV or listening to the clicks on my telephone thinking I’m wiretapped."
How susan saw it...

“I don’t know what to believe... They stalked me in my house. They told me they were watching me surf on the net. They could be doing anything. Obviously they’re capable of doing anything.”
The STATE (2): Police
Growing sophistication

“The FBI develops some hacking tools internally and purchases others from the private sector. With such technology, the bureau can remotely activate the microphones in phones running Google Inc.'s Android software to record conversations, one former U.S. official said. It can do the same to microphones in laptops without the user knowing, the person said. Google declined to comment.”

April 22, 2013:

* US Magistrate Judge Stephen Smith in Houston rules on a rarely-unsealed search warrant request featuring RAT software.

* Bank fraud and identity theft case in which “unknown persons are said to have committed these crimes using a particular e-mail account via an unknown computer at an unknown location.”

* Tool able to “search the computer’s hard drive, random access memory, and other storage media; to activate the computer’s built-in camera; to generate latitude and longitude coordinates for the computer’s location.”
Judicial pushback

Webcam spying deserves higher level of scrutiny:

“The Government’s data extraction software will activate the Target Computer’s built-in-camera and snap photographs sufficient to identify the persons using the computer. The Government couches its description of this technique in terms of ‘photo monitoring,’ as opposed to video surveillance, but this is a distinction without a difference. In between snapping photographs, the Government will have real time access to the camera’s video feed. That access amounts to video surveillance. The Fifth Circuit has described video surveillance as ‘a potentially indiscriminate and most intrusive method of surveillance.’”
Judicial pushback

Webcam spying deserves higher level of scrutiny:

“The Government’s data extraction software will activate the Target Computer’s built-in-camera and snap photographs sufficient to identify the persons using the computer. The Government couches its description of this technique in terms of ‘photo monitoring,’ as opposed to video surveillance, but this is a distinction without a difference. In between snapping photographs, the Government will have real time access to the camera’s video feed. That access amounts to video surveillance. The Fifth Circuit has described video surveillance as ‘a potentially indiscriminate and most intrusive method of surveillance.’”
judicial pushback

“What if the Target Computer is located in a public library, an Internet café, or a workplace accessible to others? What if the computer is used by family or friends uninvolved in the illegal scheme? What if the counterfeit e-mail address is used for legitimate reasons by others unconnected to the criminal conspiracy? What if the e-mail address is accessed by more than one computer, or by a cell phone and other digital devices?”
Judicial pushback

Conclusion:

“There remains a non-trivial possibility that the remote camera surveillance may well transmit images of persons not involved in the illegal activity under investigation.”
Judicial pushback

Conclusion:

“There remains a non-trivial possibility that the remote camera surveillance may well transmit images of persons not involved in the illegal activity under investigation.”

DENIED

Monday, October 21, 2013

The Government has applied for a Rule 41 warrant and security warrant targeting a computer allegedly used to violate federal laws, to steal trade secrets, and to commit securities laws. Unknown persons are said to have committed these crimes using a particular email account associated with a computer at an unknown location. The government alleges that the computer was hacked by surreptitiously installing software designed to extract certain stored data, including photos, videos, and location information over a 30 day period. In other words, the government seeks a warrant to hack a computer suspected of containing evidence. In its reasons explained below, the application is denied.

Background

In early 2013, unidentified persons gained unauthorized access to the personal email account of John Doe, an individual residing within the Southern District of Texas, and used that email address to access his bank account. The Internet Protocol (IP) address of the computer accessing Doe’s account resolves to a foreign country. After Doe discovered the breach and took steps to secure his email account, another email account nearly identical to Doe’s — the address differed by a single letter — was used to attempt a similar wire...
Remote Forensic Software

3. What is provided by the DigiTask solution?

3.1. Additional intelligence
- Audio data, e.g. from messengers
- Screenshots
- Keylogs
- File search
- Registry settings
- Remote shell
- ... (more in track 5)
“The screenshots and audio files it sends out are encrypted in an incompetent way, the commands from the control software to the trojan are even completely unencrypted. Neither the commands to the trojan nor its replies are authenticated or have their integrity protected. Not only can unauthorized third parties assume control of the infected system, but even attackers of mediocre skill level can connect to the authorities, claim to be a specific instance of the trojan, and upload fake data. It is even conceivable that the law enforcement agencies's IT infrastructure could be attacked through this channel.”
The STATE (3): Spies
We are here to save the world
AntiHacker.sytes.net

Anti Hacker
28 likes · 33 talking about this

Computers/Technology
Auto-Protect & Anti-Detect & Security & Quick scan and analysing

About

Anti Hacker shared a link.
July 27

Does HTTPS really improve Internet security compared to HTTP? How do we know that we have complete Internet Security on our devices? Get the answers in the following TechBlog post!
http://antihacker.sytes.net/index.html

http://antihacker.sytes.net/index.html

Also On

Activity
Recent
"While it purports to provide security against hackers, AntiHacker instead installs a remote access tool called DarkComet RAT, which allows an attacker to capture webcam activity, disable the notification setting for certain antivirus programs, record key strokes, steal passwords, and more. Over a dozen of the attacks EFF has analyzed have installed versions of DarkComet."
“It is with deep regret that I am here to announce the end of project DarkComet RAT after over 4 years of development, hardwork day and night to offer you for free a tool with the will to meet community's expectations for a program of type Remote Administration Tool.

Why did I take such a decision? Like it was said above because of the misuse of the tool, and unlike so many of you seem to believe I can be held responsible of your actions, and if there is something I will not tolerate is to have to pay the consequences for your mistakes and I will not cover for you.”

-Jean-Pierre Lesueur, July 2012
"Flame can gather data files, remotely change settings on computers, turn on PC microphones to record conversations, take screen shots and log instant messaging chats."

–Reuters 5/28/2012

“Flame was a highly stealthy rootkit that used the work of world-class cryptographers and mathematicians to spread from machine to machine, even on hardened networks. After infecting a system, it manipulated microphones, cameras, and Bluetooth functions to spy on people in the immediate vicinity.”
CORPORATIONS
Aaron’s

credit: Dwight Burdette/Wikimedia Commons
“After Byrd discussed the encounter with his wife Crystal, the couple recalled several recent occasions in which the computer had exhibited odd behavior... More troubling was the light next to the webcam that was inexplicably illuminated even when neither of the Byrds was shooting video or photos. The couple soon realized that for more than a month, someone had been using the laptop to remotely spy on them.”

–Ars Technica, 12/18/2012
What could Aaron’s see?
What could Aaron's see?

All of the following keys were entered:
Recording start: 12/19/2010 7:08:34 PM
[h] [o] [w] [s] [ ] [m] [i] [k] [e] [enter]

Keyboard recording stopped: 12/19/2010 7:18:50 PM

============ End of ALL Keys ===========
how often was it used?
how often was it used?

• Byrd Webcam images, screenshots, and keystrokes recorded **347 times over 11 days**, sent by e-mail to the manager of their local Aaron’s store
how often was it used?

- Byrd Webcam images, screenshots, and keystrokes recorded 347 times over 11 days, sent by e-mail to the manager of their local Aaron’s store.

- In the six months before the Byrds sued, “Detective Mode” had been installed on 650 Aaron’s computers (0.6 percent of the 92,000 total Aaron’s machines).
how often was it used?

- Byrd Webcam images, screenshots, and keystrokes recorded 347 times over 11 days, sent by e-mail to the manager of their local Aaron’s store.

- In the six months before the Byrds sued, “Detective Mode” had been installed on 650 Aaron’s computers (0.6 percent of the 92,000 total Aaron’s machines).

- But PC Rental Agent had been sold to 1,617 rent-to-own stores, and had been installed on around 420,000 computers.
how often was it used?

- Byrd Webcam images, screenshots, and keystrokes recorded 347 times over 11 days, sent by e-mail to the manager of their local Aaron’s store

- In the six months before the Byrds sued, “Detective Mode” had been installed on 650 Aaron’s computers (0.6 percent of the 92,000 total Aaron’s machines).

- But PC Rental Agent had been sold to 1,617 rent-to-own stores, and had been installed on around 420,000 computers.

- If “Detective Mode” percentages matched those at Aaron’s,
Abused?

Testimony of Chastity Hittinger, former Aaron’s sales manager at several stores:

Q. What was happening with this information that was being captured?
A. They would just basically sit back there and joke about it.

Q. Were they deleting it then?
A. No. There was actually files saved on the GM's computer of pictures.

Q. Did you ever have a chance to see those?
A: Yes.
“Keystroke logs have displayed usernames and passwords for access to e-mail accounts, social media websites, and financial institutions. Screenshots have captured additional confidential and personal information, including medical records, private emails to doctors, employment applications containing Social Security numbers, bank and credit card statements, and discussions of defense strategies in a pending lawsuit... In numerous instances, Detective Mode webcam activations have taken pictures of children, individuals not fully clothed, and couples engaged in sexual activities.”

—Federal Trade Commission
SOLUTIONS
Who's watching you through your web camera?

Protect yourself NOW with the world's best webcam cover: C-SLIDE.
SOLUTIONS

- **Black**
- **Camouflage**
- **USA Flag**
- **Gray**
- **Purple Polka Dot**
- **Fire Orange**
SOlutions

Hardware switch: Lenovo introduced one in 2010
Takeaways
Takeaways

- Powerful machines
Takeaways

- Powerful machines
- Intimate machines
Takeaways

• Powerful machines
• Intimate machines
• Networking: a two-way street
Takeaways

- Powerful machines
- Intimate machines
- Networking: a two-way street
- Changing usage patterns
Takeaways

• Powerful machines
• Intimate machines
• Networking: a two-way street
• Changing usage patterns
• Toward perfect surveillance
Takeaways

- Powerful machines
- Intimate machines
- Networking: a two-way street
- Changing usage patterns
- Toward perfect surveillance
- Ease leads to overuse
Privacy—it’s dead, Jim.
Privacy—it’s not quite dead, Jim.