CALLICOON
FINE ARTS

49 DELANCEY STREET
NEW YORK, NEW YORK
10002

Greenberg, Andy. *This Artist's Images Integrate Code From Malware Like Stuxnet and Flame*, Wired, November 27, 2014, online.

WIRED
WIRED

# This Artist's Images Integrate Code From Malware Like Stuxnet and Flame

BY ANDY GREENBERG 11.27.14

For years, sophisticated state-created malware like Stuxnet and Regin has fascinated and vexed the security research community and launched a new foreign policy debate. Now it's infecting the art world, too.

Artist James Hoff's latest series, Skywiper, integrates code from government-created malware. This one uses data from the NSA-created software Stuxnet.

In an exhibit at Manhattan's Callicoon Fine Arts gallery running through the next month, artist James Hoff is showing a new series of images that visually integrate code from government-written malware samples like Stuxnet and Flame. As Hoff describes it, he's used those spying and cyberwar tools to "glitch" the digital images. allowing the malware to add a certain uncontrollable static to his otherwise carefully crafted works of abstract color.

"It's about letting the virus be the generative aspect of the process in the studio," he says. "That variability is very interesting to me. It allows you to get out of your own way of making art and bring randomness into the mix."

Hoff creates his malware-glitched works, which have all already been sold, by dropping digital paintings into a hex editor that converts it to text. Then he intersperses randomly chosen chunks of code from malware files, and reconstitutes the data as an image file. The code corrupts the image in unexpected ways, adding chromatic streaks, blotches, and static. In two of the images, Hoff used code from the NSA-created software Stuxnet, built to destroy centrifuges at Iranian nuclear facilities. The other 14 images use code from Flame, which Hoff calls by its alternate name Skywiper, an older NSA-created spyware program.

A pair of cufflinks Hoff created that contain a USB stick that stores a piece of music whose notes are based in part on Stuxnet's code.

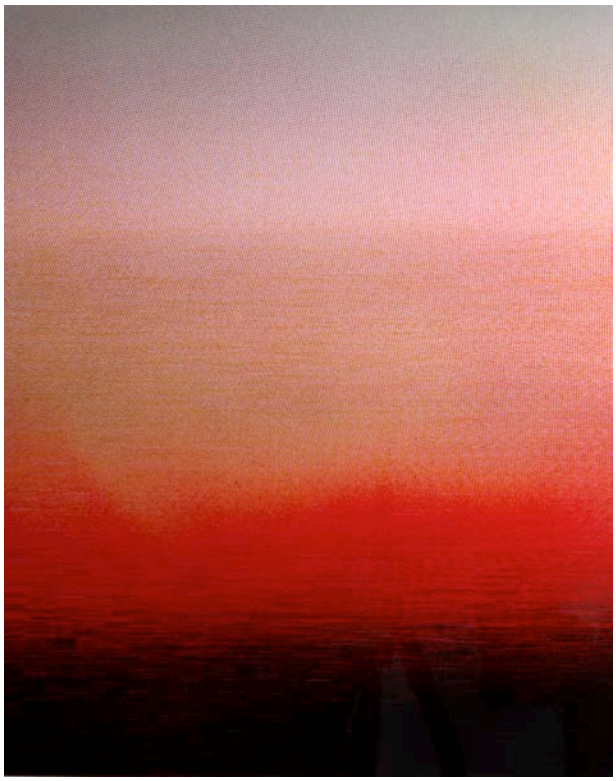
The images, which Hoff calls his Skywiper series, are only his latest malware-inspired works. Last year he created a pair of cufflinks that hid USD memory sticks that stored a piece of music based in part on Stuxnet's code. He also released a series of iPhone ringtones glitched with code from the year 2000 ILOVEYOU virus.

Despite his new focus on state-crafted malware, Hoff insists his work isn't political. But he does intend the use of state cyberwarfare tools to connect the art to the world at large. "I don't think of viruses as good or bad. To me, they're just agents," he says. "I just want to pull that element into the work. It allows for that kind of reflection, both on a conceptual level and an aesthetics level. The actual code is embedded in the image you see."

Hoff's method involves reducing a pre-created image to text with a hex editor and then "corrupting" the file with random chunks of malware code.

Other images in the series like this one use code from the NSA-created spyware tool Flame, also known as Skywiper, a name Hoff has also used for the image series.

When he reconstituted the image including the malware "glitches," they included static, streaks and blotches of color.



“I don’t think of viruses as good or bad. To me, they’re just agents,” he says. “I just want to pull that element into the work. It allows for that kind of reflection, both on a conceptual level and an aesthetics level. The actual code is embedded in the image you see.”

Hoff says he's more interested in the uncontrollable effects of adding virus code into his art than in the political aspect of government-sponsored cyberwarfare creations like Stuxnet, whose code this image uses.