DeepSec 2017 Talk: Who Hid My Desktop – Deep Dive Into hVNC – Or Safran & Pavel Asinovsky

Posted on **October 17,2017** by **sanna**

Seeing is believing. If you sit in front of your desktop and everything looks as it should look, then you are not in the Matrix, right? Right? Well, maybe. Manipulating the surface to make something to look similar is a technique also used by phishing, spammers, and social engineers. But what if the attacker sitting on your computer does not need to see what you see? Enter hidden virtual network computing where malicious software controls your system, and you don't know about it.

Since the past decade, financial institutions are increasingly faced with the problem of malware stealing hefty amounts of money by performing fraudulent fund transfers from their customers' online banking accounts. Many vendors attempt to solve this issue by developing sophisticated products for classifying or risk scoring each transaction. Often, identifying legitimate account holders is based on detecting whether the transaction is made from the legitimate user's machine or from an untrusted endpoint.

Going back 10 years, and still today, some checks are based on the IP/Geolocation of the machine performing the transaction and comparing it with the user's typical whereabouts. In order to overcome this identifier, malware authors easily turned the user's machine into a proxy, making the transaction appear to originate from the same IP address.

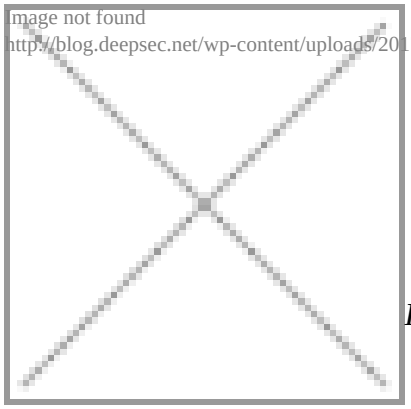
Device identification became increasingly sophisticated over the years, adding many parameters of the user's environment to fingerprint trusted devices. But cybercrime is an arms race, and malware developers did not stay behind. To completely disregard device fingerprinting, they have devised their own circumvention technique: hidden VNC (Virtual Network Computing) that enables them to commit the fraudulent transaction from the user's own machine without ever being noticed.

In this lecture, Or and Pavel will talk about hVNC in general, but also present and demo the specific use case of Gozi's proprietary hVNC tool which we reversed and broke in our labs. Gozi is one of the most advanced financial crime tools. It is operated by a cyber gang and sees constant innovation and upgrades.

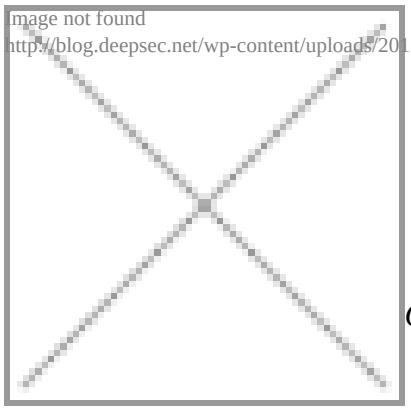
In their talk at DeepSec 2017, Pavel and Or will elaborate on the following subjects:

- What is VNC and its inherently legal uses?
- What is hVNC and why is it used in crime?
- Which financial malwares use hVNC?
- Show some of the hVNC dirty tricks and explain them.
- Explain the reversing of Gozi ISFB's hVNC module (architecture & structure).
- Live Demo [1/2] - execute the hVNC module and present a live session.
- Live Demo [2/2] - Seeing the actual fraudster session (the hidden part) - script and demo.
- Provide audience with detection/Mitigation advice.

This session is best suited for stakeholders who work in the anti-fraud departments of their organizations, malware researchers, analysts, and cybercrime investigators. The session requires basic understanding of what banking Trojans are, but does not require specific technical knowledge beyond an information security background.



Pavel Asinovsky is a malware researcher at IBM Trusteer for more than two years. Prior to that Pavel worked as a malware researcher for F5 networks and as a malware analyst at RSA-EMC. Pavel has a wide experience and interest in malware analysis.



Or Safran has been a malware researcher at IBM Trusteer for three years and holds a Bachelor of Science degree in Computer Software Engineering. Or has keen interest in hardware and software reverse engineering.

Posted in:Conference | Tagged:Cybercrime,DeepSec,Gozi,Hidden VNC,Malware,Talk | With 0 comments