CUC2005 Paper

"VF-Atak" - Virus Flood Attack

"Qubis" d.o.o.

Lucijan Caric
Tomo Sombolac 'Som'
http://www.qubis.hr
qubis@qubis.hr

Recipient: cuc@carnet.hr

Extended abstracts

"VF-ATAK" - "Virus Flood" attack

A proof-of-concept method for infecting desktop computers protected with active antivirus software with known viruses by using simple batch scripts.

These days antivirus (AV) software is a must, and there are very few companies and even home users who believe they can safely use computers in everyday work without using AV software. So, more and more users install some kind of malware protection software on their computers. And it is in our nature to believe that we are well protected if we use and continuously maintain such product, especially if it is one of several leading vendors.

But...

...unfortunately, it is not so at all. By using extremely simple and short batch script, one third party tool and Eicar virus-test file, we found out that almost every leading major AV product for desktops allowed the virus to activate at least once while AV was running and active. There are also products that allowed several dozens of activations, although we all know that it is enough for a virus to activate only once to take a complete control over computer.

"...if you have an active malware on your computer, it is not your computer any more..."

One prerequisite is really needed for VF-Atak to work - administrator level rights. It could seem that it is hard to gain such rights. However, it is not so hard - almost every home user works under admin-rights, and in our practice we noticed that surprisingly high percentage of corporate users work under administrator or admin-equal account. "...if you have just one untrusted administrator on your network, it is not your network anymore..."

So, if a malware is started under admin-rights, it could have admin rights, too. Also, in the past we have witnessed several breakouts of computer worms that either successfully gained increased rights or they found some other way to control and/or infect remote computers on network.

Also, we used some "social engineering facts" based on our everyday practice. We will show source code used in attacks.

Testing environment

We installed AV product one by one on clean Windows XP + SP2 machine (all patches were applied, too) and attacked it. Computer complied to AV vendors' system requests.

We changed only one thing after installation - we disabled automatic updates to avoid an attack during AV upgrade process.

Problems we ran into and solved

Since we are not programmers, we had to find third party tool to execute a script on victim's machine. SysInternals' PSExec, an excellent "must-have" tool, solved our problems.

First version of our scripts did not work on all AV's - our first test appeared a year ago, and AV programs evolved since. We had to evolve VF-Atak, too.

Then, some AV engines are quite fast and can easily stand one stream of viruses. So we invented a "double attack".

At least one AV program had a "nasty feature" that gave us a little headache - it blocks all communication with attacker on first occurrence of viral file. Also, in some cases we did not manage to copy Eicar to victim's computer at all. So we customized our script and forced victim to "attack itself".

Results

Results are kind of scary - at the time of writing this paper we had tested six leading AV programs and five of them allowed virus to execute.

It was not possible to infect PC in 100% of attacks, but extremely high percentage of attacks succeeds (rough approximation: 80%).

We must emphasize that these results do not have a scientific value - we don't have resources for that level of research. But these tests surely show that AV industry has to think on introducing more and different quality assurance tests to make its products stand new types of attacks.

Speakers biography

Lucijan Caric gained his LL.B. at the University of Zagreb. When he started to work in computer security and anti-virus field in 1991, he already had an extensive experience in the IT arena. He is founder and director of Qubis d.o.o., a Croatian IT security company partner of well known British security software vendor Sophos Plc. Caric is also columnist and advisor to a leading Croatian computer magazine BUG, speaker to many conferences and seminars.

Tomo Sombolac 'Som' is Support Team Leader at Qubis d.o.o, a Croatian IT security company. He came in touch with computers in the early 80's - from programming in machine code for small home computers to system engineer's responsibilities with Microsoft, Linux and Netware OS, he has constantly been connected with antivirus and security problems. His primary duty is to provide customers with as highest level of AV security as possible. Tomo presented his work on two "Virus bulletin" conferences, and published several technical articles in computer magazines.

Speaker checklist

...