



## FIRSTLIGHT EWS

### THREAT ADVISORY

January 21<sup>st</sup>, 2008

#### THREAT NAME

OleYeller.A.AntiVirus9.Symantec

#### THREAT DESCRIPTION

We have observed a new threat on the FirstLight decoy grid attempting to exploit a stack overflow present in older versions of Symantec Anti-Virus (9.x and prior). These software versions are managed through UDP port 2967. The threat makes use of a XOR decoder routine to decode its shellcode before transferring execution to it. Upon successful exploitation, the threat downloads a second stage executable. The download URI is cleverly placed outside the encoded payload to evade detection by systems that search for URIs within the encoded payload.

#### PROPAGATION

Delivery of the malware is achieved by exploiting an overflow in Symantec Anti-Virus & Symantec Client Security (CVE-2006-2630).

The executable downloaded is named svch0st.exe.

#### AV DETECTION

The second stage executable downloaded was not detected by the following anti-virus engines at the time of capture: AVG, Antivir, ClamAV, and McAfee VirusScan.

#### FIRSTLIGHT SIGNATURE COVERAGE

Infection is characterized by the following signatures triggering within a session.

`AntiVirus9.Symantec.Stack.Overflow, Xor.Countdown.Encoder.x86.A`

#### REFERENCES

<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-2630>  
<http://www.symantec.com/avcenter/security/Content/2006.05.25.html>  
<http://service1.symantec.com/SUPPORT/ent-security.nsf/pfdocs/2005033011582148?Open&dtype=corp>

#### MITIGATION

IPS devices equipped with the FirstLight signature set will block the infection vector. To mitigate the threat, users may upgrade to the latest version of Symantec AV / Client Security or block inbound UDP port 2967 traffic at the gateway.

#### FIRST CAPTURED

January 21, 2008

The FirstLight Early Warning Service detects new threats and delivers actionable intelligence to organizations interested in maintaining a proactive security posture.

Our global decoy grid solicits attack traffic to provide real-time threat intelligence including new malware, exploits, and trend information.

The FirstLight Early Warning service constantly enhances our security knowledgebase, which we translate into IPS/IDS signatures for security device vendors and enterprise customers.

For more information on the FirstLight Early Warning Service, visit us at:

<http://www.endeavorsecurity.com/flews.php>