# Endpoint Protection

symantec.com/connect/blogs/apt1-qa-attacks-comment-crew

Feb 19, 2013 05:28 PM

A L Johnson

Today Mandiant released a detailed report dubbed "APT1" which focuses on a prolific cyber espionage campaign by the Comment Crew going back to at least 2006 and targeting a broad range of industries. The report cites the earliest known public reference about APT1 infrastructure as originating from Symantec. We have detected this threat as Backdoor.Wualess since 2006 and have been actively tracking the group behind these attacks. The following Q&A briefly outlines some of the relevant Symantec information around this group:

**Q: Do Symantec and Norton products protect against threats used by this group?**

Yes. Symantec confirms protection for attacks associated with the Comment Crew through our antivirus and IPS signatures, as well as STAR malware protection technologies such as our reputation and behavior-based technologies. Symantec.cloud and Symantec Mail Security for Microsoft Exchange also detect the targeted emails used by this group.

**Q: Has Symantec been aware of the activities of the Comment Crew?**

Yes. Symantec has been actively tracking the work of the Comment Crew for a period of time to ensure that the best possible protection is in place for the different threats used by this group.

**Q: Why are they called the Comment Crew?**

They were dubbed the Comment Crew due to their use of HTML comments to hide communication to the command-and-control servers.

**Q: How does a victim get infected?**

The initial compromise occurs through a spear phishing email sent to the target. The email contains an attachment using a theme relevant to the target. Some recent examples used by this group and blocked by Symantec technologies are listed here:

- U.S. Stocks Reverse Loss as Consumer Staples, Energy Gain.zip
- Instruction_of_KC-135_share_space.doc
- New contact sheet of the AN-UYQ-100 contractors.pdf
- U.S. Department of Commerce Preliminarily Determines Chinese and Vietnamese Illegally Dumped Wind Towers in the United States.doc
- ArmyPlansConferenceOnNewGCVSolicitation.pdf
- Chinese Oil Executive Learning From Experience.doc
- My Eight-year In Bank Of America.pdf

Similar to what Symantec indicated in a recent blog, if the malicious attachment is opened, it attempts to use an exploit against the target victim's system. It drops the malicious payload as well as a clean document to keep the ruse going.

**Q: Does Symantec know who this group is targeting?**

Yes. Symantec telemetry has identified many different industries being targeted by this group including Finance, Information Technology, Aerospace, Energy, Telecommunications, Manufacturing, Transportation, Media, and Public Services. The following Figure shows a worldwide heatmap for detections related to this group since the beginning of 2012.

***Figure.*** *Heatmap of Comment Crew related detections*

**Q: Currently, what are the most prevalent threats being used by this group?**

Symantec, in the last year, has identified the most prevalent threats being used by this group as Trojan.Ecltys, Backdoor.Barkiofork, and Trojan.Downbot.

**Q: Has Symantec released any publications around these attacks?**

Yes. We have recently released publications to address techniques and targets of Trojan.Ecltys and Backdoor.Barkiofork, both of which are threats used by this group:

We have also investigated associated attacks of this group:

The Truth Behind the Shady RAT

**Q: What are the Symantec detection family names for threats used by this group?**

Symantec also detects numerous other files used by this group under various detection names:

**Q: Does Symantec have IPS protection for these threat families?**

Yes. There are several IPS signatures to catch threat families associated with this group:

**Q: How will this report affect the Comment Crew operations?**

Despite the exposure of the Comment Crew, Symantec believes they will continue their activities. We will continue to monitor activities and provide protection against these attacks. We advise customers to use the latest Symantec technologies and incorporate layered defenses to best protect against attacks by groups like the Comment Crew.