Luckycat Redux Campaign Attacks Multiple Targets in India and Japan

trendmicro.com/vinfo/us/security/news/cyber-attacks/luckycat-redux-campaign-attacks-multiple-targets-in-india-and-japan

_Download the full research paper: Luckycat Redux:

Inside an APT Campaign with Multiple Targets in India and Japan

The number of targeted attacks has dramatically increased. Unlike largely indiscriminate attacks that focus on stealing credit card and banking information associated with cybercrime, targeted attacks noticeably differ and are better characterized as “cyber espionage.” Highly targeted attacks are computer intrusions threat actors stage in rder to aggressively pursue and compromise specific targets, often leveraging social engineering, in order to maintain persistent presence within the victim’s network so they can move laterally and extract sensitive information.

In a typical targeted attack, a target receives a contextually relevant email that encourages a potential victim to click a link or open a file. The links and files the attackers send contain malicious code that exploits vulnerabilities in popular software. The exploits’ payload is a malware that is silently executed on the target’s computer. This exploitation allows the attackers to take control of and obtain data from the compromised computer. In other cases, the attackers send disguised executable files, usually compressed in archives that, if opened, also compromise the target’s computer. The malware connects back to command-and-control (C&C) servers under the attackers’ control from which they can command the compromised computer to download additional malware and tools that allow them to move laterally throughout the target’s network. These attacks are, however, not isolated “smash-and-grab” incidents but are part of consistent campaigns that aim to establish covert presence in a target’s network so that information can be extracted as needed.

Targeted attacks are rarely isolated events. In fact, they are constant. It is more useful to think of them as campaigns—a series of failed and successful attempts to compromise a target’s network over a certain period of time. The attackers, in fact, often keep track of the different attacks within a campaign in order to determine which individual attack

compromised a specific victim's network. As the attackers learn more about their targets from open source research—relying on publicly available information, as well as previous attacks, the specificity of the attacks may sharply increase.

Cyber-espionage campaigns often focus on specific industries or communities of interest in addition to a geographic focus. Different positions of visibility often yield additional sets of targets pursued by the same threat actors. We have been tracking the campaign dubbed "Luckycat" and found that in addition to targeting Indian military research institutions, as previously revealed by Symantec, the same campaign targeted entities in Japan as well as the Tibetan community.

The Luckycat campaign attacked a diverse set of targets using a variety of malware, some of which have been linked to other cyber-espionage campaigns. The attackers behind this campaign maintain a diverse set of C&C infrastructure and leverages anonymity tools to obfuscate their operations. We were able to track elements of this campaign to hackers based in China.

Luckycat Quick Profile:

First Seen:
The Luckycat campaign has been active since at least June 2011.

Victims and Targets:
The Luckycat campaign has been linked to 90 attacks against the following industries and/or communities in Japan and India:

- Aerospace
- Energy
- Engineering
- Shipping
- Military research
- Tibetan activists

Operations:

- Targeted emails that are contextually relevant (i.e., emails containing a decoy document of radiation dose measurement results sent some time after the Great East Japan Earthquake
- Exploited CVE-2010-3333 (aka, Rich Text Format [RTF] Stack Buffer Overflow Vulnerability) in several instances, although Adobe Reader and Flash Player vulnerabilities were also exploited
- Used TROJ_WIMMIE or VBS_WIMMIE—malware that take advantage of the Windows Management Instrumentation (WMI), making the backdoor component undetectable through file scanning

- The WIMMIE malware, once inside the network, connects to a command-and-control (C&C) server via HTTP over port 80
- Attackers heavily used free web-hosting services but also used virtual private servers (VPSs) for more stable operations

Possible Indicators of Compromise
WIMMIE malware do not leave much network fingerprint. However, the following is an identifiable HTTP C&C communication fingerprint—count.php?m=c&n=[HOSTNAME]_[MAC_ADDRESS]_[CAMPAIGN_CODE]@. This format can also be seen in the URL inside the script when /namespace:\\root\subscription path __eventconsumer is typed in the command line for WMI.

Relationship with Other APT Campaigns
Malware identified with the ShadowNet, Duojeen, Sparksrv, and Comfoo campaigns were used or found hosted on the same dedicated server used by the LuckyCat campaign.

** The campaign codes we have seen so far are detailed in the Trend Micro research paper, "Luckycat Redux: Inside an APT Campaign with Multiple Targets in India and Japan." The characteristics highlighted in this APT campaign profile reflect the results of our investigation as of March 2012*

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cyber Attacks, Research, Targeted Attacks, Vulnerability Research