Clever Kitten | Threat Actor Profile

crowdstrike.com/blog/whois-clever-kitten/

April 4, 2013

Who is Clever Kitten

April 4, 2013

Adam Meyers Research & Threat Intel

Over the last several weeks, CrowdStrike has been discussing some of the dozens of adversaries that the CrowdStrike Intelligence team tracks every day. We revealed a Chinese-based adversary we crypt as Anchor Panda, a group with very specific tactics, techniques, and procedures (TTPs) and a keen interest in maritime operations and naval and aerospace technology. Last week we discussed Numbered Panda, a group that is also based out of China and is fairly well known to the security community, though by many names. The goal in discussing that group was to illuminate the issues with the varied naming systems for characterizing attackers. This week we want to make sure that we draw attention to the fact that there are adversaries active in computer network exploitation besides those with a nexus to China.

Targeted attackers who are are not fulfilling a protracted collection requirement often go unnoticed by the larger security community. These adversaries conduct more discreet or less-visible operations; this makes their presence and activities more difficult to catch. The adversary we are focusing on this week fits into this category, and in fact has very little to do with the objectives of the People’s Republic of China. This week we are going to discuss **Clever Kitten, whom, by virtue of several indicators, we have affiliated with the Islamic Republic of Iran.** Clever Kitten primarily targets global companies with strategic importance to countries that are contrary to Iranian interests.

Clever Kitten actors have **a strong affinity for PHP server-side attacks to make access**; this is relatively unique amongst targeted attackers who often favor targeting a specific individual at a specific organization using social engineering. Some attackers have moved to leveraging strategic web compromises. The reason for this is likely the availability of exploits against web browsers, which for a variety of reasons allows an attacker to bypass security features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR).

The technical details of these protections and subsequent bypasses is not the subject of this post, and there are many great blogs and white papers available on that subject. This is not to say other adversaries do not target web servers, but that **this adversary seems to favor targeting web servers**.

Clever Kitten’s Methods

RECONNAISSANCE

A Clever Kitten attack starts with the use of a web vulnerability scanner to conduct reconnaissance. The scanner they favor was identified by artifacts left in web logs on victimized servers. The scanner was identified as the Acunetix Web Vulnerability Scanner which is a commercial penetration testing tool that is readily available as a 14-day trial. Clever Kitten unabashedly audits publicly facing websites looking for an exploitable page.

INSTALLATION

Once an exploitable page is identified, the actor will attempt to upload a PHP backdoor to gain remote access to the system. The PHP backdoor observed in these attacks is RC SHELL v2.0.2011.1009, which is publicly available. This adversary encrypts the backdoor and wraps it with an AES-256-bit function containing a password that decrypts the file when the script is executed.

ACTIONS AND OBJECTIVES

In commodity-based attacks, the intent after the machine is compromised generally revolves around stealing data from a database, uploading an exploit kit to deliver drive-by attacks, or simple defacement. In Clever Kitten’s attacks, the goal is lateral movement; this is an attempt to move further into the target environment in order to begin intelligence collection. This activity is a longer tail for the actor than a spearphish; this is likely based on the Clever Kitten background, which may be focused on web development/application testing.

In order to move laterally, Clever Kitten may leverage additional vulnerability scanners or reconnaissance tools, but almost always will use a packet-sniffing utility in an attempt to capture a login credential or network-based traffic that can be used to move deeper into the victim organization. Clever Kitten's goal is to eventually be able to masquerade as a legitimate user by compromising credentials either through a pass-the-hash attack, or by dumping password hashes from a compromised host. Once these credentials are compromised, Clever Kitten will authenticate as a legitimate user and slip into the noise of regular user authentications.

Unfortunately, as we are still very much investigating Clever Kitten and their TTPs, the Intelligence Gain/Loss equation dictates that we not share too many indicators of these attacks at this time. We decided to highlight Clever Kitten for two reasons. The first is that this adversary is not attributed to PRC, which we believe is important to occasionally highlight, as it is not the only computer espionage actor.

Without going too deep into the rabbit hole, there are several indicators pointing to an Iranian nexus, including language artifacts in the tool-marks used by the attacker, as well as network activity tying this actor to a very specific location that we have high confidence in not being spoofed. The second reason for highlighting Clever Kitten is that this is a rare situation where we have the ability to provide an indicator around the reconnaissance phase of the adversaries' activity.

Reconnaissance is frequently the hardest activity to identify and alert on by nature of the fact that targeted attackers may spend weeks or months reconnoitering a target, and by the time the attack is detected and responded to, that data is not available for correlation, or it is so innocuous that it is impossible to tease out of logs.

The first Snort IDS rule provided below will detect Accunetix web scans, which, while in and of themselves are NOT indicative of Clever Kitten activity, may help organizations identify web scans that may relate to a more serious problem. The second rule addresses the RC SHELL response that is sent from the victim in nearly every response to the attacker. The CrowdStrike Intelligence team received some great community feedback from the previous rule releases and will continue to use this feedback to deliver quality rules that can enable actionable intelligence.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"[CrowdStrike] - Acunetix scan"; flow: established, from_client; content:"GET /acunetix-wvs-test-for-some-inexistent-file"; depth: 47; sid: XXX; rev: 1; )
```

```
alert tcp $HTTP_SERVERS any -> $EXTERNAL_NET any (msg: "[CrowdStrike] - RC Webshell Victim Enumeration Table Header"; content: "SYS</td>|0a|<td align="center" class="topt">|0a|KERNEL</td>|0a|<td align="center"
class="topt">|0a|USER</td>|0a|<td align="center" class="topt">|0a|DISK
TOTAL/FREE</td>"; flow: established, from_server; sid: xxx; rev: 1;)
```

Other Iranian-based Adversaries

- Helix Kitten

Curious about other nation-state adversaries? *Visit our threat actor center to learn about the new adversaries that the CrowdStrike team discovers.*

Be sure to follow @CrowdStrike on Twitter as we continue to provide more intelligence and adversaries over the coming weeks. If you have any questions about these signatures or want to hear more about Clever Kitten and their tradecraft, please contact: intelligence@crowdstrike.com and inquire about our intelligence-as-a-service solutions.

Related Content

Who is EMBER BEAR?

A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell