Operation Earth Kitsune - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Earth Kitsune

Names	Operation Earth Kitsune *(Trend Micro)*	
Country	North Korea	
Motivation	Information theft and espionage	
First seen	2019	
Description	(Trend Micro) We previously wrote about the SLUB malware in 2019, noting that it abused (among others) Slack and GitHub as part of its routine. Its previous campaigns used watering hole tactics as an infection vector, using websites that discussed topics related to North Korea. Our continuous monitoring of this threat campaign shows that the threat actor behind SLUB didn't stop their attacks even during the pandemic. In 2020, we found multiple instances of their attacks in March, May, and September, delivering a new variant of the malware — this time incorporating new techniques and capabilities. In addition, we found two unknown malware variants delivered along with SLUB during the latest attack at the end of September. Besides the CVEs already mentioned in the previous SLUB blog, we also found new exploits for the vulnerabilities CVE-2016-0189, CVE-2019-1458, CVE-2020-0674, and CVE-2019-5782, chained with another Chrome bug that does not have an associated CVE. The campaign is very diversified, deploying numerous samples to the victim machines and using multiple command-and-control (C&C) servers during this operation. In total, we found the campaign using five C&C servers, seven samples, and exploits for four N-day bugs. The scale of the attack and the samples' custom design suggest that there is a group behind this operation. We dubbed the campaign as Operation Earth Kitsune.	
Observed	Countries: Worldwide except South Korea.	
Tools used	agfSpy, dneSpy, SLUB, WhiskerSpy.	
Operations performed	Late 2022	Earth Kitsune Delivers New WhiskerSpy Backdoor via Watering Hole Attack

		<https://www.trendmicro.com/en_us/research/23/b/earth-kitsune-delivers-new-whiskerspy-backdoor.html>
Information	<https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-kitsune.pdf>	

Last change to this card: 25 April 2023

Download this actor card in PDF or JSON format
