Operation LagTime IT: colourful Panda footprint

Published: 2021-01-08 · Archived: 2026-04-05 12:37:11 UTC

Presented at the VB2020 localhost conference, 30 September - October 2, 2020. ↓ Conference paper: https://vb2020.vblocalhost.com/upload... ↓ Slides: https://vb2020.vblocalhost.com/upload... → Details: https://vb2020.vblocalhost.com/presen... ✪ PRESENTED BY ✪ • Fumio Ozawa (NTT Security) • Shogo Hayashi (NTT Security) • Rintaro Koike (NTT Security) ✪ ABSTRACT ✪ Operation LagTime IT by TA428 is an attack campaign targeting govermental organizations of East Asian countries reported by Proofpoint in July 2019. It is still in the wild and actively working as of 2020. We successfully unveiled and grasped the whole attack picture, including how TA428 interacts with a target, through detailed research on two samples (document file on Qasem Soleimani and COVID-19) observed in January and February 2020. The existing research results on Operation LagTime IT only reported that it used Royal Road RTF Weaponizer, Poison Ivy and Cotx RAT. But according to the behaviour that we observed, TA428 also performed user environment checking, credential stealing, lateral movement and highly sophisticated defense evasion. In this presentation, we describe the operational steps that TA428 has taken from initial samples to reaching the deepest part of victim system. We also reveal the analysis result of the malware used by TA428 and the codes that decode encrypted communication. Because it is estimated that the techniques, tools and malware used in Operation LagTIme IT have similarity or relations with other various APT actors, we discuss how they overlap. Through this presentation, SOC, CSIRT and security researchers will be able to have deeper understanding of Operation LagTime IT and gain knowledge on how to detect or defend against the attack. ✪ BIO: Fumio Ozawa (NTT Security) ✪ Fumio Ozawa is a security analyst at NTT Security (Japan) KK, where he runs malware and exploit analysis, and the SOC operation. Now he focuses on APT threat analysis and hunting. He has spoken at the Japan Security Analyst Conference 2018 hosted by JPCERT/CC. He has written some white papers about the banking trojan Ursnif and APT watering hole attacks in Japanese. ✪ BIO: Shogo Hayashi (NTT Security) ✪ Shogo Hayashi has worked as a SOC analyst for more than 10 years at NTT Security (Japan) KK. His main specialization is responding to EDR detections, creating IoCs, malware analysis and researching endpoint behaviour of threat actors. In addition, he posts articles and whitepapers in NTT Security. He is a cofounder of SOCYETI, an organization for sharing threat information and analysis technique to SOC analysts in Japan. ✪ BIO: Rintaro Koike (NTT Security) ✪ Rintaro Koike is a security analyst at NTT Security (Japan) KK. He has been engaged in SOC and malware analysis. In addition, he is the founder of 'nao_sec'. He always collects and analyses threat information. He has been a speaker at Japan Security Analyst Conference 2018/19/20, HITCON Community 2019, VB 2019, AVAR 2019, CPRCon 2020 and Black Hat USA 2018 Arsenal.
