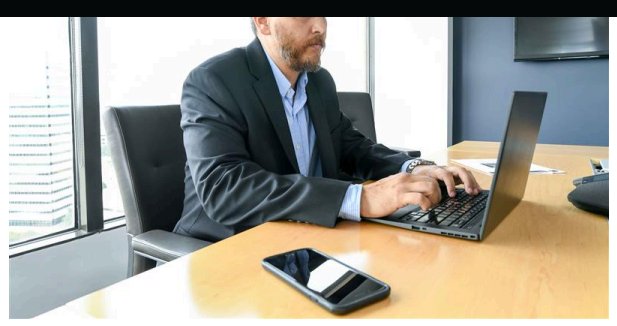
Malicious Spam Campaign Uses ISO Image Files to Deliver LokiBot and NanoCore

June 28, 2019

surprising to see more unusual file types being employed as file attachments, as was the case with an April campaign discovered by Netskope that used ISO image files to deliver two notorious Trojans: LokiBot and NanoCore.



The malicious spam comes in the form of a fake invoice email which states that the recipient can access the billing by opening an ISO image attachment. This is notable because invoices are usually sent as Word documents or Excel files. Thus, the use of an ISO image as an invoice is highly unusual. Adding to the suspicious nature of the attachment is the file size. Samples were roughly 1MB to 2MB — again uncommon given that typical ISO images tend to have larger file sizes.

Contained within the image is the executable payload —either LokiBot (detected as TrojanSpy.Win32.LOKI.THFBFAI) or NanoCore (detected as Backdoor.Win32.NANOBOT.SMY)— which is downloaded onto the system when a user clicks on the attachment.

The technique used in this campaign confirms that cybercriminals are using a larger variety of file types for their email attacks. Trend Micro detections of advanced email threats in 2018 included malware-ridden spam with IQY and ARJ file attachments. ISO files are automatically mounted upon clicking, and email security solutions usually whitelist it, so it makes sense that cybercriminals are experimenting with its use.

[Read: Trend Micro Cloud App Security Report 2018: Advanced Defenses for Advanced Email Threats]

LokiBot and NanoCore

LokiBot is a sophisticated malware family that has information stealing and keylogging capabilities. Often advertised in the underground as a tool used for stealing passwords and cryptocurrency wallets, it has extensively been used in a wide variety of campaigns.

The variant used in this particular campaign has a number of capabilities that help it detect where it is loaded. It uses the function IsDebuggerPresent() to detect if it is running inside a debugger and it also measures the computational time difference between CloseHandle() and GetProcessHeap() to check if it is running inside a virtual machine. In addition to gathering data, which includes web browser information and login credentials, it also checks for the presence of web and email servers as well as remote administration tools.

The other payload, NanoCore, is a Remote Access Tool (RAT) that has high modularity and customizability thanks to various plugins which expand its capabilities.

Like LokiBot, it is sold in underground forums, making it available for other threat actors to use in their own attacks. In this malspam campaign, NanoCore creates a mutual exclusion object (mutex), performs process injection, and uses the registry for persistence. Similar to the LokiBot payload, it also tries to detect the presence of a debugger. The goal of NanoCore is to capture clipboard data and keystrokes and steal information from document files.

- Email Threat Landscape Report: Cybercriminal Tactics, Techniques That Organizations Need to Know
- Trend Micro Cloud App Security Threat Report 2021
- A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report
- Securing the Pandemic-Disrupted Workplace: Trend Micro 2020 Midyear Cybersecurity Report
- Australian Health Insurance-Themed Spam Spreads Ursnif

Recent Posts

- Cellular IoT Vulnerabilities: Another Door to Cellular Networks
- Ransomware Spotlight: INC
- The Realities of Quantum Machine Learning
- Unchaining Blockchain Security Part 3: Exploring the Threats Associated with Private Blockchain Adoption
- Generative AI in Elections: Beyond Political Disruption

While both LokiBot and NanoCore are fairly advanced malware, malspam is their primary delivery method. Therefore, best practices for detecting and preventing malicious emails remain effective in helping users avoid malware.

- **Be wary of grammatical and typographical errors.** Business emails, especially communications between a business and its suppliers, will usually be written in a professional manner. An email that contains blatant grammatical or typographical errors could be a sign that it is a malicious email.
- **Double check the email address of the sender.** The easiest way to determine if an email is authentic is to check the sender's email address. If it doesn't use the official domain of the sender's organization, or uses an unusual email, that's a red flag.
- **Context, context, context.** If the email content fails to provide context regarding the discussion (such as a one-liner) and also includes a link or an attachment, then there is a high chance that it is a malspam attempt.
- **Don't click or download.** Even if an email looks legitimate, it's still prudent to avoid clicking on any links or downloading any files until the source is verified to be legitimate. Hacked email accounts have previously been used for spear phishing.

Trend Micro email security solutions powered by machine learning

To make it easier for organizations to protect their employees from phishing and advanced email threats, they can consider email protection like the Trend Micro™ Cloud App Security™ solution, which uses machine learning (ML) to help detect and block attempts at spam and phishing. It can detect suspicious content in the message body and attachments as well as provides sandbox malware analysis and document exploit detection.

Posted in Cybercrime & Digital Threats, Spam

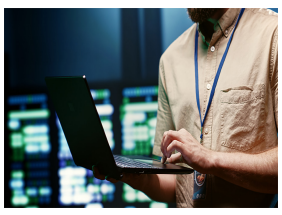
Internet of Things

Cellular IoT Vulnerabilities: Another Door to Cellular Networks

UNWIRED: Understanding the Unforeseen Risks in Evolving Communication Channels

MQTT and M2M: Do You Know Who Owns Your Machine's Data?

Virtualization & Cloud



Today's Cloud and Container Misconfigurations Are Tomorrow's Critical Vulnerabilities

Uncover Cloud Attacks with Trend Vision One and CloudTrail

Kong API Gateway Misconfigurations: An API Gateway Security Case Study

Ransomware

Ransomware Spotlight: INC

Phobos Emerges as a Formidable Threat in Q1 2024, LockBit Stays in the Top Spot: Ransomware in Q1 2024

Ransomware Spotlight: LockBit

Security Technology

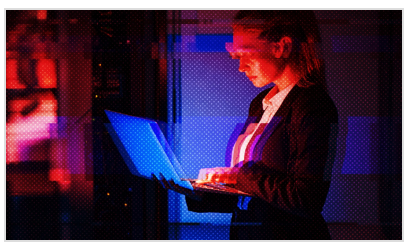
The Realities of Quantum Machine Learning

API Security Exposed: The Role of API Vulnerabilities in Real-World Data Breaches

Post-Quantum Cryptography: Migrating to Quantum Resistant Cryptography

View the 2024 Trend Micro Security Predictions

Calibrating Expansion: 2023 Annual Cybersecurity Report



View the report

Try our services free for 30 days

Start your free trial today

Country Headquarters

Trend Micro - Hong Kong (HK)

903-905 9/F Shui On Centre, 6-8 Harbour Road Wanchai, Hong Kong

Phone: +852-2214-3200

Copyright ©2024 Trend Micro Incorporated. All rights reserved