January 8, 2025

Lessons from a Malspam Hunt

Spoofed Domains to Bypass Safeguards

Despite security safeguards, malicious spam still pays off. To get beyond controls, threat actors fake or spoof an email's sender address to make it appear more legitimate.

In recent research, Infoblox Threat Intel analyzed spam sent from a Chinese actor named Muddling Meerkat, a mysterious actor conducting DNS operations via the Chinese Great Firewall. The exercise discovered multiple malicious spam campaigns and the widespread usage of domain spoofing.

Hunting ingredients: homegrown telemetry and community feedback

While questions remained after our initial publication on Muddling Meerkat, we shared what we knew and reached out to the larger community for additional comments. Received feedback included in-depth abuse notification reports caused by large-scale spam distribution, pointing to a Chinese Source IP, and Infoblox owned some of the abused domains.

With this knowledge in mind, Infoblox Threat Intel started a hunt correlating our own DNS authoritative name server logs with data collected from spam traps. By pivoting back and forth between all data, we intended to learn more about the breadth of Muddling Meerkat malspam operations. This led to additional insights into the usage of malspam conducted by related China-linked actors. Here are four key observations obtained:

Catch #1: QR Code Phishing Campaigns

The largest group of malspam evolved around phishing campaigns targeting residents of greater China. These campaigns spoof old domains and distribute attachments containing QR codes that lead to phishing sites. The attackers employ a two-step method where recipients open the email attachment first and then use WhatsApp to scan the QR code. This methodology complicates security measures by moving the interaction to an encrypted chat app, which is out of sight of most security tools. In the second step, the threat actors also used registered domain generation algorithms (RDGAs) to create random domains that are active for only a brief period to further evade detections.

Catch #2: Japanese Phishing Campaigns

A sizable percentage of collected spam originated from sources with three-letter hostnames. By grouping these, we discovered a malspam operation targeting Japanese users. This campaign involved emails referencing popular brands like Electronic Toll Collection (ETC), Sumitomo Mitsui Banking Corporation (SMBC), Amazon, and Mastercard. The emails urged users to authenticate due to security concerns, leading them to a traffic distribution system (TDS) and eventually to fake login pages that steal credentials.

Another campaign targeted Japanese users with spam messages related to MyEtherWallet, a popular crypto wallet. These messages used lookalike domains and sometimes included Japanese text, asking users to log in to their accounts. Although the links appeared legitimate, they led to fake domains created by the threat actors.

The use of fake domains, domain spoofing and TDSs all indicate how these Chinese actors apply multiple tactics to stay out of the threat research spotlight and evade detection.

Catch #3: Familiar Extortion Campaigns

We also found campaigns using well-known spam tactics that featured domain spoofing. One common tactic involved extortion emails claiming that a hacker had accessed the user's device and recorded embarrassing activities. These emails spoofed the user's email address, making it appear that the user sent the message from their own account. The email demanded payment in Bitcoin to remove the malware, with the amount varying across messages. Despite the surprising nature of these emails, the scam is effective, as some Bitcoin wallets associated with these campaigns contained significant funds. These campaigns, and others using spoofed sender domains, likely originate from lingering spam bots rather than the work of sophisticated actors such as Muddling Meerkat.

Catch #4: Mysterious Malspam

The research uncovered a mysterious and active spam campaign using spoofed sender domains and benign Excel spreadsheet attachments with no evident purpose. These emails, which spoof domains like those used by Muddling Meerkat, come from a Chinese freight company. The email addresses vary widely and include synthetic usernames like "Edward.Evelyn" and "Heidi.Gracie." The campaigns were observed every two out of three days in 2024, with subject lines indicating new freight rate updates, however, no malicious content was found in these files.

Interestingly, the emails also do not include a call to action and are just a continually updated set of freight rates for a Chinese shipping company. Domain spoofing removes any sense of legitimacy, making it unclear why either a shipping company or a malicious actor would send such emails.

A similar technique was seen in personal spam, where emails provided mutual fund values from an Indian investment company. These messages, flagged by Google Mail as suspicious spam, also contained an innocuous spreadsheet and a PDF file. In this case, the sender's username was a former acquaintance, suggesting their email account was hacked for spam operations. However, the value of these messages for the spam actor remains unclear.

Takeaway: Domain Spoofing is a Widely Used Tactic

When we first published Muddling Meerkat in March 2024, we identified about 20 related domains but now have confirmed several hundred others discovered in spam traps. Unfortunately, we were not able to correlate them back to our own DNS authoritative name server logs, leaving a mystery about the actor.

While we were unable to determine what Muddling Meerkat is up to, our investigation was successful in that we learned a great deal about how actors use spoofed domains in malspam, which can inform ways to stop them. For threat researchers like us, that insight is often every bit as important as knowing all the intentions behind them.

Download **the latest report** and explore how Infoblox Threat Intel analyzed spam campaigns originating from behind the Great Chinese Firewall.