Over 120 Malicious Domains Discovered in Analysis on New Roaming Mantis Campaign

Archived: 2026-04-02 11:24:24 UTC

November 19, 2018 • Ofir Ashman

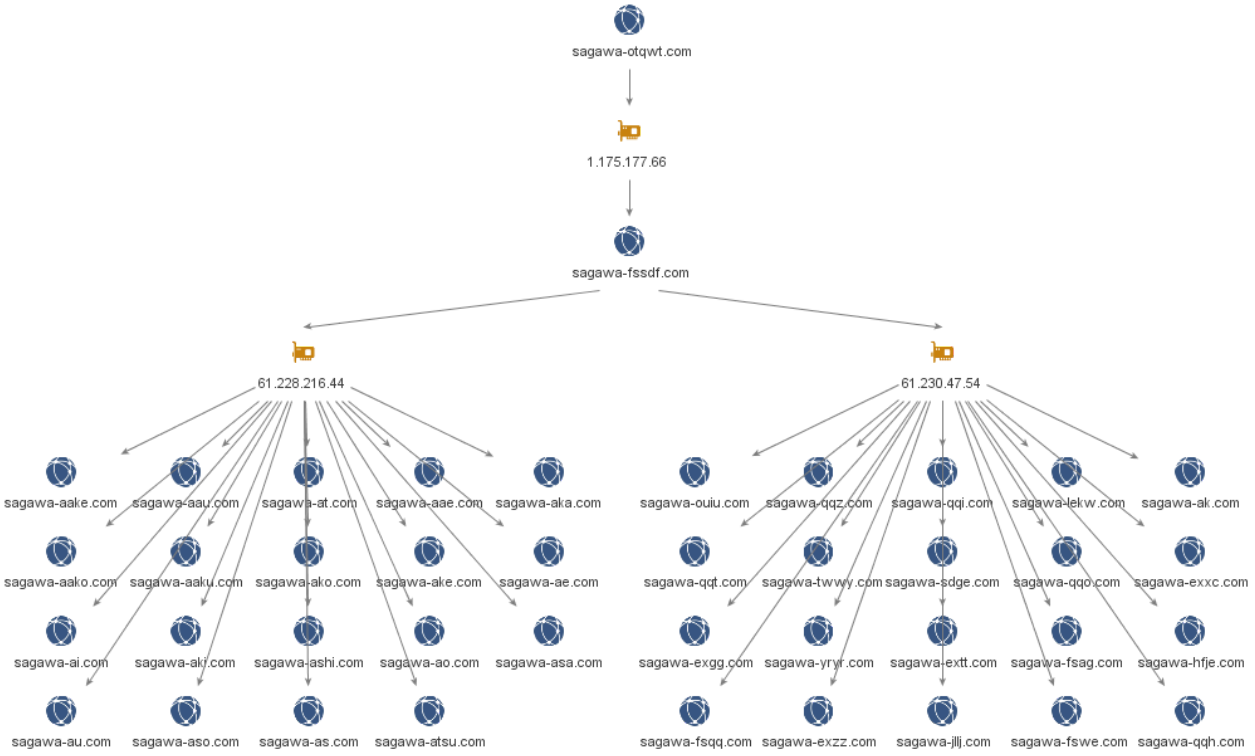
Since April of this year, news of a rapidly evolving crypto mining malware, dubbed Roaming Mantis, has hit the cyber news headlines. Roaming Mantis debuted with a DNS hijacking attack vector, infecting android running machines. Once installed, the malware redirected infected devices to phishing sites by spoofing legitimate applications, while using the stolen credentials to run a crypto mining script on PCs.

Recently, Securelist researchers uncovered a new Roaming Mantis infection vector targeting android running machines. The attack starts with a phishing SMS including malicious link which, when clicked, redirects users to a website where the malicious Sagawa APK is downloaded.

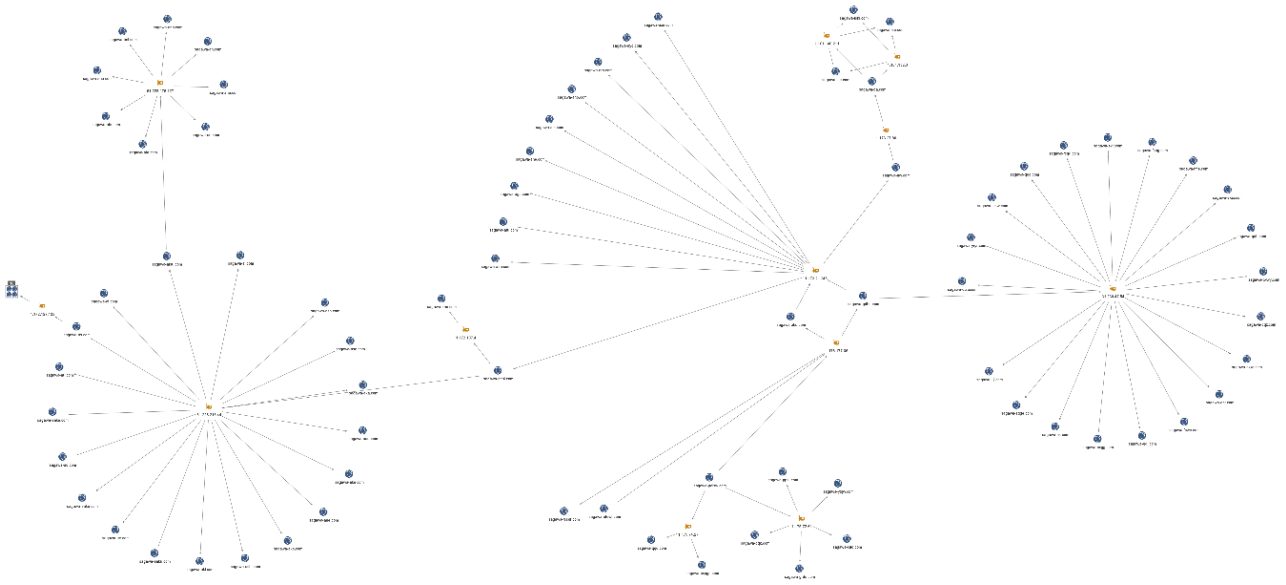
During the ThreatSTOP Security Team's analysis of indicators of compromise for this campaign, we noticed a pattern in domain syntax linking a published domain to many other presumably malicious domains.

In the Securelist publication, two domains were published as malicious hosts for Roaming Mantis. One domain, sagawa-otqwt[.]com, was discovered still active and hosted on the IP 1[.]175[.]177[.]66. When looking at the IP's resolve history, we found that it had recently hosted a similar-looking domain - sagawa-fssdf[.]com.

Upon further examination, we uncovered that this domain had previously been hosted on two other IPs, 61[.]230[.]47[.]54 and 61[.]228[.]216[.]44, which had hosted many other “sagawa” domains. The syntax is similar between all domains, starting with the string “sagawa-,” followed by 3-5 letters and the .com TLD.



By performing similar domain-IP-domain resolves on the domains hosted on the two IPs mentioned above, we were able to find many more “sagawa” domains:



This analysis has provided ThreatSTOP with over 120 new indicators related to Sagawa APK, and possibly also to Roaming Mantis. We are continuing this analysis, and will continue protecting our customers from Sagawa APK and Roaming Mantis.

Want to learn more? Plus, actually see what's being blocked on your network? Try out ThreatSTOP for 14 days (for free) here.

Source: https://blog.threatstop.com/over-120-malicious-domains-discovered-in-analysis-on-new-roaming-mantis-campaign