The new NotCompatible: Sophisticated and evasive threat harbors the potential to compromise enterprise networks

By Tim Strazzere

Archived: 2026-11-24 02:01:15 UTC

November 19, 2014

Over the past two years, Lookout has tracked the evolution of NotCompatible. It was a compelling threat from the start, marking one of the first times hacked websites were used at a large scale to specifically target and infect mobile devices.

NotCompatible.C has set a new bar for mobile malware sophistication and operational complexity. The command infrastructure and communication perseveres and self-protects through redundancy and encryption, making it elusive and enduring. It's an earthworm with its tail cut off that regenerates and thrives.

The technological evolution of NotCompatible has turned a once compelling piece of malware into one of the known longest-running mobile botnets we've seen to-date. This malware is a prime example of how mobile malware complexity is advancing and is borrowing technical tactics already seen in PC malware.

NotCompatible is used as a proxy to run spam campaigns or scalp concert tickets. While NotCompatible.A was relatively simplistic architecturally, NotCompatible.C is a changed beast in terms of the technological concepts it uses to stay alive.

Our investigation, shows the possibility that a threat like this could expand to assist in attacks on corporate networks, a risk that should not be ignored. Lookout has thus far actively protected against NotCompatible on hundreds of thousands of devices in the U.S. and around the world.

NotCompatible Malware USA_Encounter rate

Notcompatible Malware Europe_encounter rate

Mobile malware campaign sophistication at PC levels

In NotCompatible.C we see technological innovation in a mobile malware system that reaches the levels more traditionally displayed by PC-based cybercriminals.

In 2012, when Lookout first detected NotCompatible.A, the threat acted as a simple proxy on infected devices. Fast forward to 2014 and the emergence of the new "C" variant of NotCompatible — the technology has significantly matured though the usage has remained the same. NotCompatible.C is ultimately a botnet-for-rent; though the server architecture, peer-to-peer communications, and encryption make it a much more formidable threat. NotCompatible.C's use of encryption and peer-to-peer communication mirror advanced PC threats such as later Conficker. Much like later variants of Conficker, these features of NotCompatible.C would make it more

difficult to detect and stop at the network level due to the obfuscation of its communications and the interchangeability of its endpoints.

Because of its sophistication, NotCompatible has become the longest running mobile botnet we've ever observed, in operation since 2012. Take, for comparison, another mobile botnet we found in 2012 called SpamSoldier. It infected phones for the purpose of sending spam SMS messages without the user's consent. However, because it didn't have the same technological maturity, we were able to work with carriers and have the botnet taken down within weeks.

Server architecture and operations


NotCompatible Operations

Traditionally mobile malware operators have not done so much to protect their infrastructure or communications. NotCompatible.C, however, employs a two-tiered server architecture. The gateway command and control (C2) server uses a load balancing approach, in which infected devices from different IP address regions are filtered and segmented geographically, and only authenticated clients are allowed to connect. Not only does this model bring client usage efficiency, our research suggests that it also aids in avoidance of discovery. We suspect that the gateway C2 makes it difficult for behavioral analysis systems and researchers to pick up on traffic.

If an infected device validates with the gateway properly, it will receive a configuration file containing all active operational C2s, which, at last count, comprised more than ten separate and distinct servers located across Sweden, Poland, Netherlands, the U.K., and the U.S.

Client connections

Once contact has been made with the operational C2, the infected device receives a list of other infected devices (i.e. "clients") to which the it can connect with and share intel.

Herein lies a massive strength of NotCompatible.C.

This capability to allow a client to receive C2 connection orders through any number of clients creates a powerful redundancy — effectively a contingency plan — in the NotCompatible ecosystem and hardens itself against disruption. Thanks to the peers, the client can easily find new C2s even if steps are taken to bring down the C2s to which it initially connected.

End-to-end encryption

Unlike NotCompatible.A, all communications between the clients and C2s are encrypted. NotCompatible.C's traffic will appear as binary data streams, unremarkable and indistinguishable from legitimate encrypted traffic such as SSL, SSH or, VPN traffic.

The rent-a-botnet business

NotCompatible is very likely a rent-a-botnet business that allows anyone to buy access for a variety of activities.

Through observing the proxy usage and commands from the C2s Lookout has tracked a few distinct malicious uses of NotCompatible.C, including:

- Spam campaigns (Live, Aol, Yahoo, Comcast)
- Bulk ticket purchasing (Ticketmaster, Livenation, Eventshopper, Craigslist)
- Bruteforce attacks (WordPress)
- c99 shell control (observed logging into shells and performing different actions)

In order to gain new clients to add to this business, the NotCompatible.C operators use the same distribution methods as earlier variants — drive-by downloads through spam campaigns and compromised websites.

NotCompatible.C operators do not use any exploits that we know of and instead rely on social engineering tactics to trick victims into completing installation of the malware. One observed spam email informs the user that they need to install a “security patch” in order to view an attached file.

It appears that the malware operators have also bought compromised accounts and websites in bulk. For example, Lookout has observed spam campaigns tied to specific groups of compromised accounts: in one campaign they were all AOL accounts, in another, all Yahoo accounts.

Risk to protected networks


NotCompatible Attack Patterns

To date, Lookout has not observed NotCompatible.C being used to target protected networks, though the proxy capability makes it a potential threat as well as a direct risk to network security. We believe that NotCompatible is already present on many corporate networks because we have observed, via Lookout’s userbase, hundreds of corporate networks with devices that have encountered NotCompatible.

How could this threat make its way into an organization? As soon as a device carrying NotCompatible.C is brought into an organization on a mobile device, it could provide the operators of this botnet with access to the organization’s network. Using the NotCompatible proxy, an attacker could potentially do anything from enumerating vulnerable hosts inside the network, to exploiting vulnerabilities and search for exposed data.

In our investigation, you’ll find protection strategies which consumers and enterprises can take including endpoint security and segmentation of the corporate network.

Where there is a business demand, there is often an advancement in technology. It’s clear that customers of NotCompatible’s mobile botnet have found it to be useful; likely spurring the creators to make this a robust and difficult to cut down operation. We expect more of this type of sophistication in mobile malware. Mobile malware maturity is here.

Source: https://web.archive.org/web/20160605032711if_/https://blog.lookout.com/blog/2014/11/19/notcompatible/