ThreatCloud Intelligence Analysis:

It's Alive: The Resurgence of ZeroAccess Botnet

2 April 2014

Check Point Malware Research Group

Summary

Through leveraging Check Point's ThreatCloud security intelligence, in recent weeks, our vulnerability research team has detected a spike in ZeroAccess botnet activity. This is surprising given that this botnet was taken down by law enforcement, working in conjunction with Microsoft, in mid-December 2013.

Despite this enforcement action, it appears that the criminals behind ZeroAccess have simply picked up where they left off. Further, the latest Check Point research indicates that organizations may not be doing enough to prevent and remove known bots from their networks.

About ZeroAccess

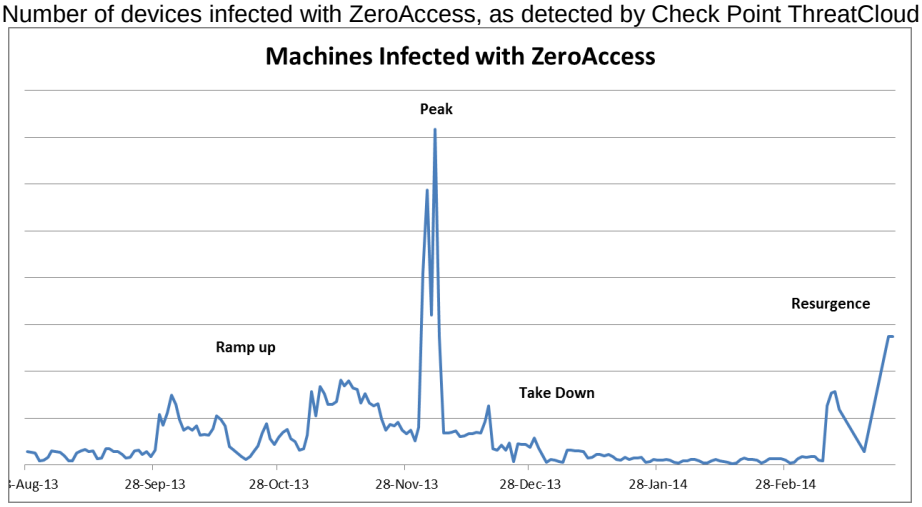
Initially discovered in February 2012, this worm enables remote code execution and malware downloads. The botnet is spread through drive-by downloads on malicious sites, fake blogs, fake Torrent files, P2P file-sharing applications, instant messaging (IM) applications and more. It has been known to update itself through peer-to-peer networks, making it possible for the authors to improve it and potentially add new functionality.

Although Microsoft and law enforcement agencies worked diligently to track down the IP addresses of the ZeroAccess botnet's command and control (C&C) network, they never fully resolved the issue of removing these bots from infected computers. The bots have now found a new way to communicate with C&C servers.

Analysis

Check Point ThreatCloud monitors the ZeroAccess bot by watching the number of organizations and number of devices that are infected with it. Just before the takedown in December 2013, ThreatCloud detected a peak in the number of infected machines – tracking thousands of infected devices worldwide. For the 3 months following the takedown, ThreatCloud detected a very low number of devices infected with the ZeroAccess bot. All that changed in early March of this year– the ZeroAccess bot has risen again.

Number of devices infected with ZeroAccess, as detected by Check Point ThreatCloud

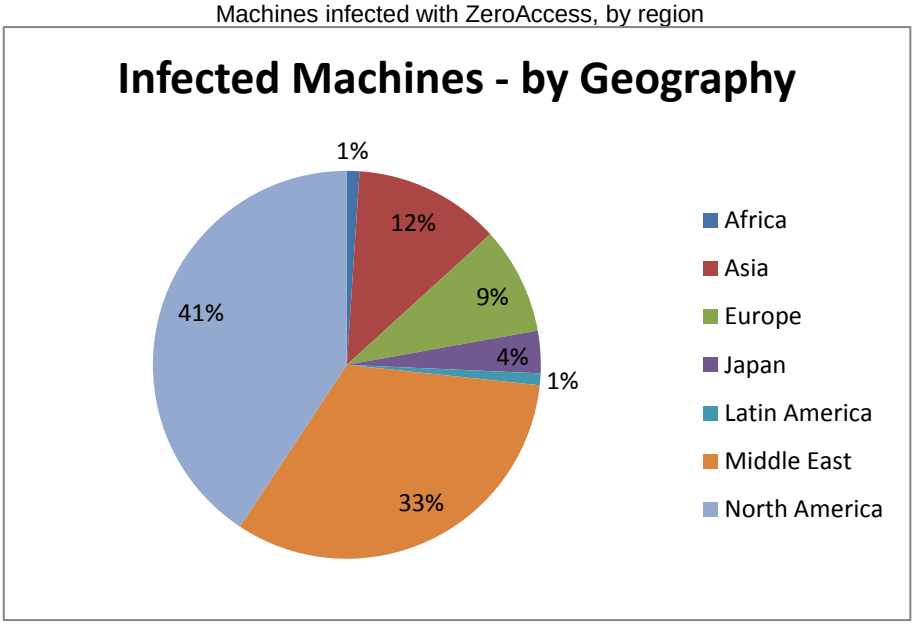


ZeroAccess bot isn't isolated; it's global

The ZeroAccess bot attacks on a worldwide basis. According to Check Point research, ZeroAccess is present on all continents, in 75 different countries.

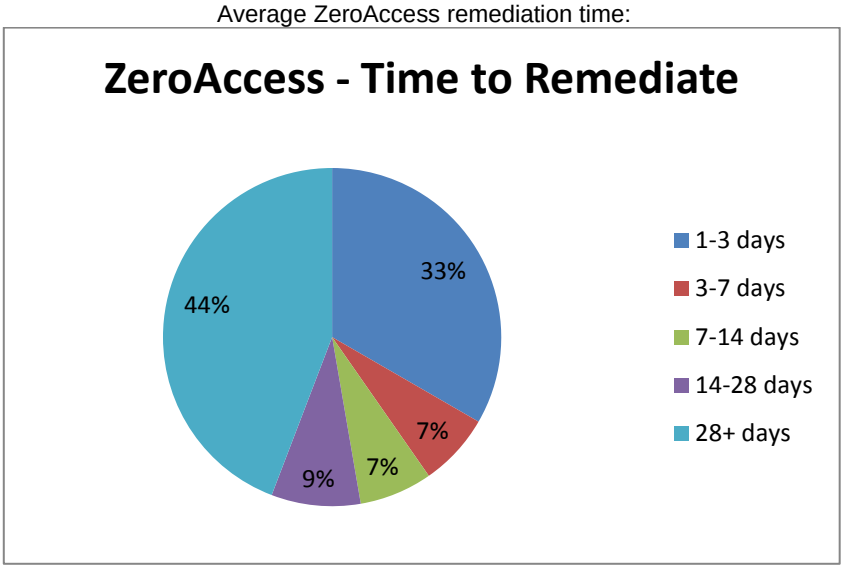
Forty-one percent of the infected devices are located in North America, followed by 31% from the Middle East. 12% of the C&C communications originated in Asia, followed by Europe (9%), Japan (4%) and Latin America (1%)

Machines infected with ZeroAccess, by region



Organizations aren't cleaning up ZeroAccess quickly
Almost half of the organizations worldwide (44%) wait up to four weeks or longer before taking action to clean ZeroAccess, according to Check Point research. Despite the ZeroAccess bot remaining unchanged, ThreatCloud data shows that only 33% of organizations clean ZeroAccess infected devices within the first 3 days of detection. Although organizations have the ability to know that they are infected, they chose not to remediate those devices, putting their organizations at risk.

Average ZeroAccess remediation time:



Conclusion: Bots can and will come back, so protect your organization

Check Point's monitoring of ZeroAccess over the past months shows that bots in the wild still survive. Even bot networks that have been "taken down" can be built back up. Check Point customers should enable the Anti-Bot Software Blade to identify and detect communication of bots, prevent communications to C&C and provide alerts when such activities are detected.

Check Point will continue to follow up on ZeroAccess, providing protections to its customers through Threat Prevention technologies and ThreatCloud.