Novel Malware Persistence Within ESXi Hypervisors

Greetings,

HC3 has been made aware of an ongoing novel malware ecosystem impacting VMware ESXi, Linux vCenter servers, and Windows virtual machines based on a Mandiant blog post (Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors ?????), and additional reporting. HC3 analysts assess that working exploits are being leveraged for these vulnerabilities, and additional exploits are highly likely to become available soon. It is recommended that Healthcare and Public Health (HPH) organizations using ESXi and the VMware infrastructure suite follow the hardening steps outlined in this Mandiant blog post to minimize the attack surface of ESXi hosts.

Regards,

The HC3 Team

If you have any additional questions, have feedback, or wish to join our distribution list for updates, email us at HC3@hhs.gov.

To view our archive of resources, visit our website at www.HHS.gov/HC3.