Cyber Threat Advisory CTA-2016-02.1-POS_Multigrain

CTA | 3 May, 2016

Point of Sales (POS) Evolution to DNS Exfiltration

The Multigrain Point of Sales (POS) malware highlights the need for protection against DNS-based data exfiltration and the critical need for Infoblox DNS Threat Analytics protection. Multigrain POS malware was identified by and published publicly on April 17, 2016 from the Visa Threat Intelligence and FireEye partnership program. This discovery identified a single malware sample used to scrape memory for credit card numbers and exfiltrate recovered credit card information via DNS tunneling. This single malware sample used the embedded domain datavhg[.]com to exfiltrate data from active POS systems. This form of data exfiltration is likely to increase in the future because of its effectiveness at circumventing traditional firewall appliances. Infoblox DNS Threat Analytics successfully detected the reported datavhg[.]com domain's malicious activities five months earlier on the day the malware became active on November 17, 2015. Additionally, our protection platform detected a second domain, likely used by the same threat actor, which went active a few days prior on November 14, 2015. This sister domain, dojfgj[.]com, was active and remained undiscovered by traditional threat intelligence groups until Infoblox's Cyber Intelligence Group associated the domain's activity through existing telemetry on April 22, 2016. The malicious nameservers used to receive the credit card data were hosted on dedicated hosting services provided by Vultr and Choopa. The perpetrator controlling these nameservers registered both domains via eNom Inc. and received domain protection from Whoisguard Inc.

Mitigations from Infoblox:

Infoblox customers can purchase Infoblox DNS Threat Analytics, the industry-first platform that uses streaming analytics to discover DNS-based data exfiltration. This product works in conjunction with the DNS Firewall to prevent DNS data exfiltration in real-time. Our analytics platform detected the Multigrain malware data exfiltration and would have provided subscribers an option to block upon detection and alert incident response teams to start an investigation. Infoblox DNS Firewall will protect against known threats of POS malware command and control infrastructure.

- Infoblox DNS Threat Analytics would have shortened the discovery of infection from nearly 5 months down to the day of infection.
- Infoblox DNS Firewall leverages Cyber Intelligence research to block POS system attacks before they start.