LevelBlue - Open Threat Exchange

By TheNewRaikage

Archived: 2026-04-05 21:04:59 UTC

Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

What is Multigrain? Learn what makes this PoS malware different.

BY PANDALABS • AUGUST 4, 2016 | Multigrain is a Point of Sale (PoS) malware that specializes in stealing credit and debit card information while using RAM-Scraping techniques (it directly accesses the RAM memory from certain processes to obtain the information from the cards). This has become a popular method as international laws prohibit this information from being stored on the disk (not even temporarily). Another characteristic of Multigrain is that it uses DNS petitions in order to communicate with the outside (and so it can send the stolen information). In this article we will analyze the malware itself as well as the way the malware communicates.

- 144 Subscribers

- 72 Subscribers

PosCardStealer and Large-scale Attacks Jeopardize PoS Systems

BY LUIS CORRONS • AUGUST 9, 2016 | Some weeks ago we unveiled an attack that affected hundreds of restaurants in the United States using a malware called PunkeyPOS. Something that we did not disclose is how we discovered PunkeyPOS: it turns out that we've actually been investigating a series of PoS (Point of Sale) attacks that have also affected hundreds of bars, restaurants and stores in the US. While we were analyzing one of these attacked systems, it was attacked by yet another cybergang using PunkeyPOS. In this article we are going to discuss this attack that we are still investigating that uses a PoS malware called PosCardStealer.

- 144 Subscribers

MULTIGRAIN – POINT OF SALE

FileHash-MD5: 1 | **Domain:** 1

FireEye recently discovered a new variant of a point of sale (POS) malware family known as NewPosThings. This variant, which we call "MULTIGRAIN", consists largely of a subset of slightly modified code from NewPosThings. The variant is highly targeted, digitally signed, and exfiltrates stolen payment card data over DNS. The addition of DNS-based exfiltration is new for this malware family; however, other POS malware families such as BernhardPOS and FrameworkPOS have used this technique in the past. Using DNS for data exfiltration provides several advantages to the attacker. Sensitive environments that process card data will often monitor, restrict, or entirely block the HTTP or FTP traffic often used for exfiltration in other environments. While these common internet protocols may be disabled within a restrictive card processing environment, DNS is still necessary to resolve hostnames within the corporate environment and is unlikely to be blocked.

- 374,006 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:multigrain