FIN7 Dissected: Hackers Accelerate Pace of Innovation

blog.morphisec.com/fin7-attack-modifications-revealed

- Tweet
-

PLEASE DOWNLOAD THE DETAILED ATTACK ANALYSIS IN PDF HERE

Like clockwork, FIN7 again unleashed a new attack able to bypass almost every security solution. The attack, which took place between October 8 to 10, 2017, is yet another demonstration of the high-paced innovation by threat actors.

FIN7 is one of today's most organized and sophisticated cybercrime groups, primarily known for targeting US businesses to steal payment card data. They typically use clever, customized spear-phishing lures with malicious attachments. Once an organization is infected, they move laterally across the network, using various anti-forensic techniques to evade detection. The group is closely tied to the notorious Carbanak Gang, responsible for a slew of attacks against financial institutions, although so far evidence falls short of directly equating the two.

Over the past year, Morphisec has been closely monitoring FIN7 and their targets, publishing several analyses on methods used by this group. In June 2017 Morphisec identified a highly sophisticated fileless attack targeting restaurants across the US, as discussed on Morphisec's blog and in a post co-authored with Cisco Talos. The June campaign used a new stealer DLL variant injected into malicious documents.

In this report we take a broader approach, describing in detail the rapid dynamic changes over the course of the last four months, including the recent October attack, which was first documented by researchers at Icebrg. We examine each of the component modifications in

the attack chains, and show how those changes helped FIN7 evade the dynamic behavior patterns and static patterns applied by many security solutions.

In fact, a presentation on FIN7 by FireEye at this year's InfoSecurity Europe stated that "In most environments, prevention is not possible." The presenters, however, did not take into account the effectiveness of Moving Target Defense solutions (e.g. Morphisec Endpoint Threat Prevention solution) against these types of attacks.

The technical analyses, **available for download here**, discusses:

- DOCUMENT STRUCTURE
- STAGE 1: LNK FILE – OLE OBJECT
- LNK FILE – PROPERTIES CODE CONTENT
- LNK FILE – FILE DETAILS / BATCH FILE DETAILS
- STAGE 2 – OLE AUTOMATION
- SHAPE.TEXTFRAME.TEXT
- STAGE 3 – SCHEDULED TASKS
- STAGE 4 – NETWORK BASED DETECTION EVASION
- STAGE 5 - POWERSHELL – REFLECTIVE DLL INJECTION

YOU CAN DOWNLOAD THE PDF OF THE DETAILED REPORT HERE.

Contact SalesInquire via Azure