# Operation Groundbait: Espionage in Ukrainian war zones

welivesecurity.com/2016/05/18/groundbait

May 18, 2016

After BlackEnergy and Operation Potao Express, ESET researchers have uncovered another cyberespionage operation in Ukraine: Operation Groundbait.

In addition to the armed conflict in eastern Ukraine, in recent years the country has been facing a significantly higher number of targeted cyberattacks, or so-called advanced persistent threats (APTs).

After BlackEnergy, which has, most infamously, facilitated attacks that resulted in power outages for hundreds of thousands of Ukrainian civilians, and Operation Potao Express, where attackers went after sensitive TrueCrypt-protected data from high value targets, ESET researchers have uncovered another cyberespionage operation in Ukraine: Operation Groundbait.

## Cyber-surveillance focusing on separatists

The main point that sets Operation Groundbait apart from the other attacks is that it has mostly been targeting anti-government separatists in the self-declared Donetsk and Luhansk People's Republics.

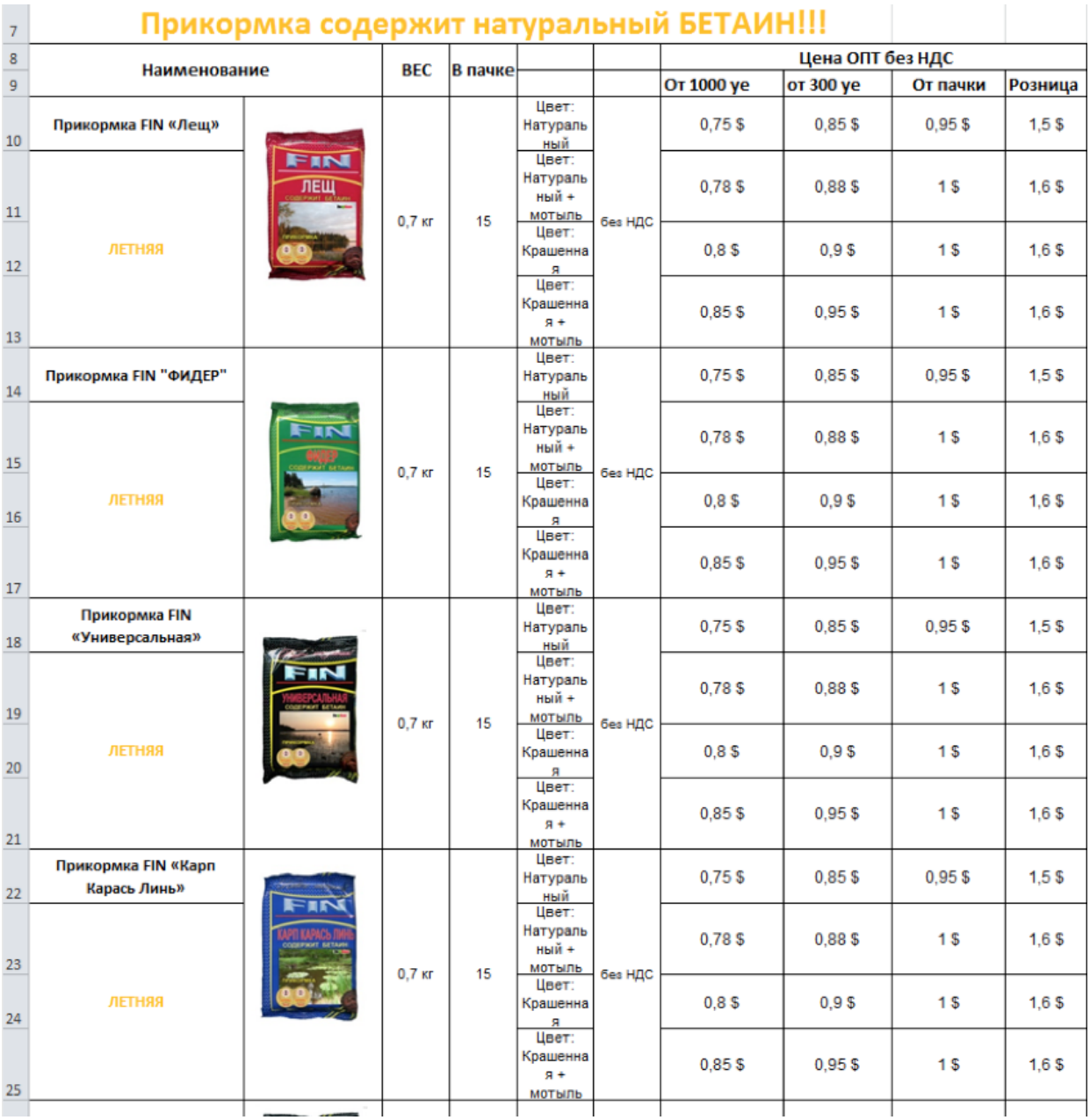
While the attackers seem to be more interested in separatists and the self-declared governments in eastern Ukrainian war zones, there have also been a large number of other targets, including, among others, Ukrainian government officials, politicians and journalists..

## Groundbait?

These cyberespionage activities have been carried out using a malware family that ESET detects as *Win32/Prikormka*. The malware has until now eluded the attention of anti-malware researchers since at least 2008.

The infection vector for spreading the malware was mostly through spear-phishing emails (which is somewhat the norm for targeted attacks). During our research, we have observed a large number of samples, each with its designated campaign ID, an appealing file name to spark the target's interest, and decoy documents with various themes related to the current Ukrainian geopolitical situation and the war in Donbass.

We chose the name Groundbait – the translation of the Russian word Prikormka (*Прикормка*) – because of a puzzling theme used in one campaign that stood out among the others, which used themes related to the armed conflict. The malware file name was prikormka.exe and it displayed a pricelist of fishing groundbait, a choice of decoy document that we have so far been unable to explain.



Прикормка содержит натуральный БЕТАИН!!!

| Наименование | | ВЕС | В пачке | | | Цена ОПТ без НДС | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | От 1000 уе | от 300 уе | От пачки | Розница |
| Прикормка FIN «Лещ» |  | 0,7 кг | 15 | Цвет: Натуральный | без НДС | 0,75 $ | 0,85 $ | 0,95 $ | 1,5 $ |
| ЛЕТНЯЯ | | | | Цвет: Натуральный + мотыль | | 0,78 $ | 0,88 $ | 1 $ | 1,6 $ |
| | | | | Цвет: Крашенная | | 0,8 $ | 0,9 $ | 1 $ | 1,6 $ |
| | | | | Цвет: Крашенная + мотыль | | 0,85 $ | 0,95 $ | 1 $ | 1,6 $ |
| Прикормка FIN "ФИДЕР" |  | 0,7 кг | 15 | Цвет: Натуральный | без НДС | 0,75 $ | 0,85 $ | 0,95 $ | 1,5 $ |
| ЛЕТНЯЯ | | | | Цвет: Натуральный + мотыль | | 0,78 $ | 0,88 $ | 1 $ | 1,6 $ |
| | | | | Цвет: Крашенная | | 0,8 $ | 0,9 $ | 1 $ | 1,6 $ |
| | | | | Цвет: Крашенная + мотыль | | 0,85 $ | 0,95 $ | 1 $ | 1,6 $ |
| Прикормка FIN «Универсальная» |  | 0,7 кг | 15 | Цвет: Натуральный | без НДС | 0,75 $ | 0,85 $ | 0,95 $ | 1,5 $ |
| ЛЕТНЯЯ | | | | Цвет: Натуральный + мотыль | | 0,78 $ | 0,88 $ | 1 $ | 1,6 $ |
| | | | | Цвет: Крашенная | | 0,8 $ | 0,9 $ | 1 $ | 1,6 $ |
| | | | | Цвет: Крашенная + мотыль | | 0,85 $ | 0,95 $ | 1 $ | 1,6 $ |
| Прикормка FIN «Карп Карась Линь» |  | 0,7 кг | 15 | Цвет: Натуральный | без НДС | 0,75 $ | 0,85 $ | 0,95 $ | 1,5 $ |
| ЛЕТНЯЯ | | | | Цвет: Натуральный + мотыль | | 0,78 $ | 0,88 $ | 1 $ | 1,6 $ |
| | | | | Цвет: Крашенная | | 0,8 $ | 0,9 $ | 1 $ | 1,6 $ |
| | | | | Цвет: Крашенная + мотыль | | 0,85 $ | 0,95 $ | 1 $ | 1,6 $ |

Figure 1 – Decoy document with groundbait pricelist

From a technical perspective, the malware features a modular architecture, allowing the attackers to expand its functionality and steal various types of sensitive information and files from the cyber-surveillance targets.

Further technical details of the malware, as well as additional information on the ongoing cyberespionage operation, can be found in our comprehensive whitepaper.

## So who's behind it?

As is usual in the world of cybercrime and APTs, attributing the source of the attack is tricky as conclusive evidence is difficult to find. Our research into the attacks has shown that the attackers most likely operate from within Ukraine.

Whoever they are, based on the types of targets chosen – mostly separatists in the self-declared Donetsk and Luhansk People's Republics – it is probably fair to assume that this cyber-surveillance operation is politically motivated.

Apart from that, any further attempt at attribution would at this point be speculative. It is important to note that in addition to separatists, the targets of this campaign include Ukrainian government officials, politicians and journalists. The possibility of false flags must be considered too.

Our comprehensive whitepaper includes more information on the Operation Groundbait campaigns and technical details of the Prikormka malware. Indicators of Compromise (IOC) that can be used to identify an infection can also be found in the whitepaper or on github.

For any inquiries, or to make sample submissions related to the subject, contact us at: threatintel@eset.com

18 May 2016 - 02:30PM