Операція Groundbait («Прикормка»): Аналіз інструментарію спостереження

АНТОН ЧЕРЕПАНОВ, ESET

Зміст

Основні положення

Операція Groundbait («Прикормка») є поточною операцією кіберспостереження за окремими особами в Україні. Група зловмисників, задіяна в операції, запустила цілеспрямовану і, можливо, політично мотивовану атаку для шпигування за наперед визначеними жертвами.

У даній статті представлені результати операції Groundbait на основі досліджень спеціалістів ESET сімейства шкідливих програм Prikormka. В матеріал включений детальний технічний аналіз цього виду загроз та механізми їх поширення, а також опис найбільш значних кампаній атак.

Основні висновки:

- Найбільшу кількість шкідливих програм було зафіксовано в Україні. Загрози розпочали свою активну діяльність не пізніше 2008 року.
- В основному операція Groundbait направлена на антиурядових представників самопроголошених Донецької та Луганської Народних Республік Східної України.
- Серед інших мішеней кіберзлочинців — українські державні урядовці, політики, журналісти, а також інші відомства.
- Цілком імовірно, що зловмисники працюють на території України.

Виявлення

У третьому кварталі 2015 року спеціалісти ESET виявили раніше невідоме модульне сімейство шкідливих програм – Prikormka. Подальші дослідження показали, що дана загроза почала поширюватися щонайменше з 2008 року. За період активності найбільше шкідливих програм зафіксовано в Україні. Тривалий час Prikormka залишалася непоміченою через відносно низьке співвідношення загроз до 2015 року. Однак у минулому році кількість даного небезпечного програмного забезпечення суттєво зросла.

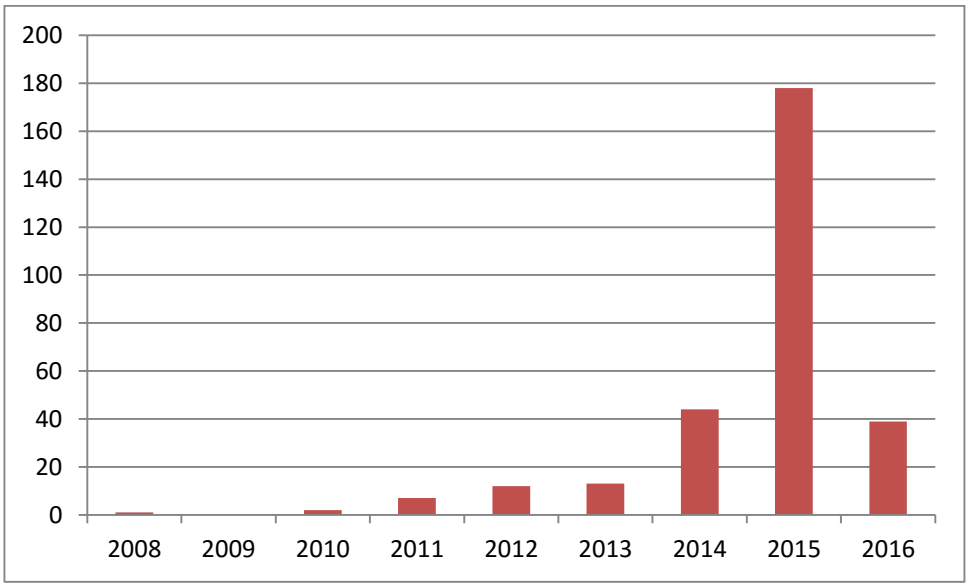


Рис. 1. Кількість унікальних зразків, виявлених ESET на основі тимчасових міток, по роках

На Рис. 1 показано кількість унікальних зразків Prikormka, зібраних за кожен рік, починаючи з 2008 року, відповідно до часових відміток заголовків PE. Як відомо, часові відмітки не є надійним показником, тому в даному випадку їх точність була підтверджена даними, отриманими за допомогою хмарних технологій ESET LiveGrid®.

Один з перших прикладів такого шкідливого програмного забезпечення, який проаналізували спеціалісти в лабораторії ESET, став `prikormka.exe`. Взагалі слово «прикормка» означає тип наживки, який кидають у воду для заманювання риби. Оскільки шкідливе програмне забезпечення поширювалося з назвою Win32/Prikormka та Win64/Prikormka відповідно, спеціалісти стали використовували цю кодову назву в своєму дослідженні, а згодом вирішили залишити її надалі.

Низький коефіцієнт виявлення та здатність залишатися непоміченими протягом багатьох років є спільною характеристикою цілеспрямованих атак (APTs). Дослідження кампаній та діяльності Prikormka підтвердило використання даної шкідливої програми під час цілеспрямованих атак.

Взагалі цілеспрямовані атаки здійснюються з різною метою, зокрема для розвідки, крадіжки інтелектуальної власності, диверсій та шпигунства. Після аналізу тактики, методів і процедур, які використовуються групою шкідливих програм Prikormka, спеціалісти ESET виявили, що мішенями кіберзлочинців ставали окремі особи, а не компанії. Навіть у випадку виявлення загрози в корпоративному середовищі не було зафіксовано жодних бокових рухів — метод, який використовується для здійснення передових кібер-атак.

Спеціалісти ESET підозрюють, що група кіберзлочинців працює в Україні, де перебуває більшість жертв зловмисників. Враховуючи це та характер атак, дії зловмисників класифіковано як операції кіберспостереження.

Кампанії

У цьому розділі подані найбільш значущі та визначні кампанії, а також документи-приманки, які використовувались для їх здійснення.

Нижче подана статистика виявлення загроз в деяких країнах на основі даних ESET LiveGrid®:

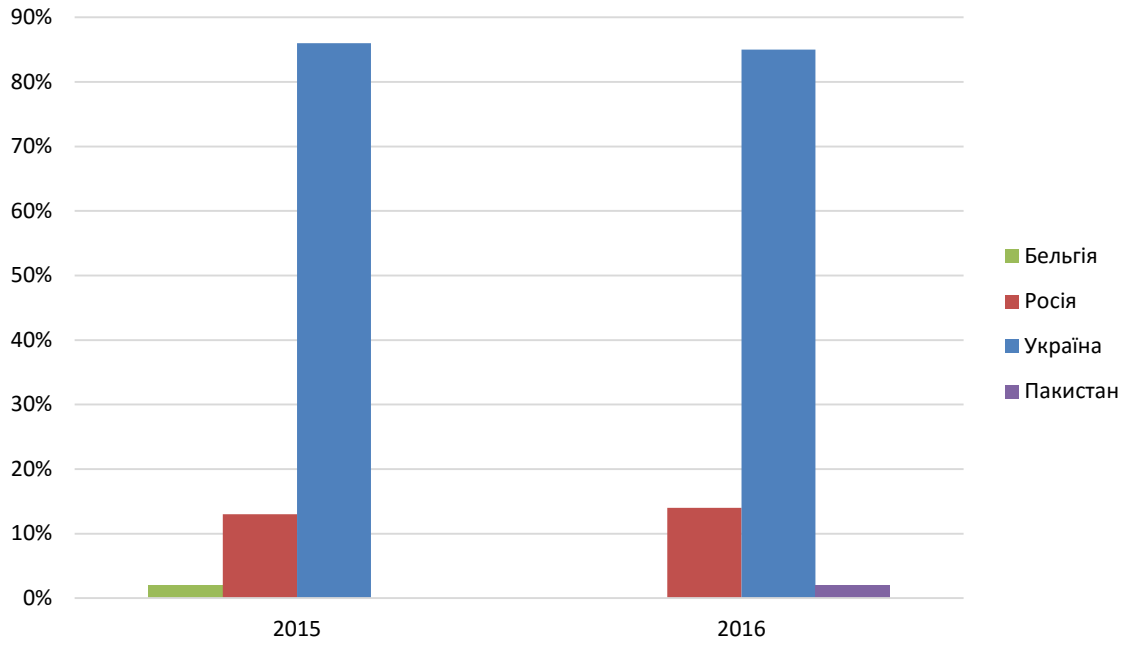


Рис. 2. Статистика виявлення шкідливих програм Prikormka відповідно до ESET LiveGrid®

Відповідно до отриманих даних, найбільша кількість виявлень шкідливої програми зафіксована в Україні. Крім того, зловмисники демонструють вільне володіння українською та російською мовами, а також повне розуміння поточної політичної ситуації в Україні.

Для отримання даних про жертви, які були атаковані в зазначених вище країнах, спеціалісти ESET проаналізували документи-приманки, які використовували кіберзлочинці для поширення загроз.

Основним способом інфікування, який був визначений спеціалістами ESET в ході дослідження, стало поширення фішингових електронних листів з прикріпленими шкідливими файлами або з посиланнями для завантаження небезпечного файлу, розміщеного на віддаленому сервері. Після відкриття замаскованого небезпечного вкладення, Prikormka відображає документ-приманку для обману та відволікання уваги потенційної жертви, яка очікує безпосередньо відкриття документу, не підозрюючи про загрозу. Цей метод спрацьовує у випадках, коли користувачі не є технічно обізнаними та не дотримуються правил безпеки під час роботи за комп'ютером. Але в той же час успіх процесу зараження найбільше залежить від якості фішингових листів. Зловмисник має більше шансів інфікувати комп'ютер у разі, якщо фішингові повідомлення та документи-приманки стосуються жертви та не викликають її здивування щодо отримання листа з подібним змістом. Таким чином, аналіз таких документів-приманок може надати інформацію про передбачувані цілі даних кібератак.

Крім цього, існує ще один артефакт, вбудований в кожен зразок шкідливої програми Prikormka, який спеціалісти ESET називають ID кампанії. Це унікальні текстові рядки, які оператори небезпечних програм використовують для ідентифікації конкретних інфекцій або спроб зараження. Використані комбінації букв і цифр іноді можуть надати інформацію про визначені зловмисниками цілі.

На даний час спеціалісти ESET виявили більше 80 різних ID кампанії та значно більше документів-приманок, пов'язаних з даними ідентифікаторами. Як правило, один ID кампанії використовується для однієї цілі, в ролі яко може бути фізична особа, юридична особа чи група людей. Це означає, що один певний ID може бути виявлений на багатьох комп'ютерах.

Більш повний перелік типових кампаній разом з компіляцією їх часових відміток та унікальних ID кампаній подані у Додатку 1 даного документу.

Варто відзначити, що в деяких випадках важко визначити потенційних жертв, особливо у разі виявлення зараження шкідливим програмним забезпеченням Prikormka після його встановлення та початку активності. Проте спеціалістам ESET стало відомо про деякі активні загрози Prikormka у комп'ютерних мережах важливих структур, зокрема українського уряду. Інші визначні цілі наведені в подальших описах кампаній Groundbait.

Кампанії проти представників окупованих територій

Однією з основних мішеней Prikormka стали представники окупованих територій Східної України. Починаючи з 2014 року на цій частині території України розгортається збройний військовий конфлікт.

У квітні 2014 року група людей в односторонньому порядку проголосила незалежність двох областей Східної України: Донецької та Луганської. У відповідь на дії окремих активістів український уряд класифікував їх терористичними організаціями, а територія областей була оголошена зоною Антитерористичної операції (АТО). 11 травня 2014 року самопроголошена влада республік провела референдум для узаконення створення республік.

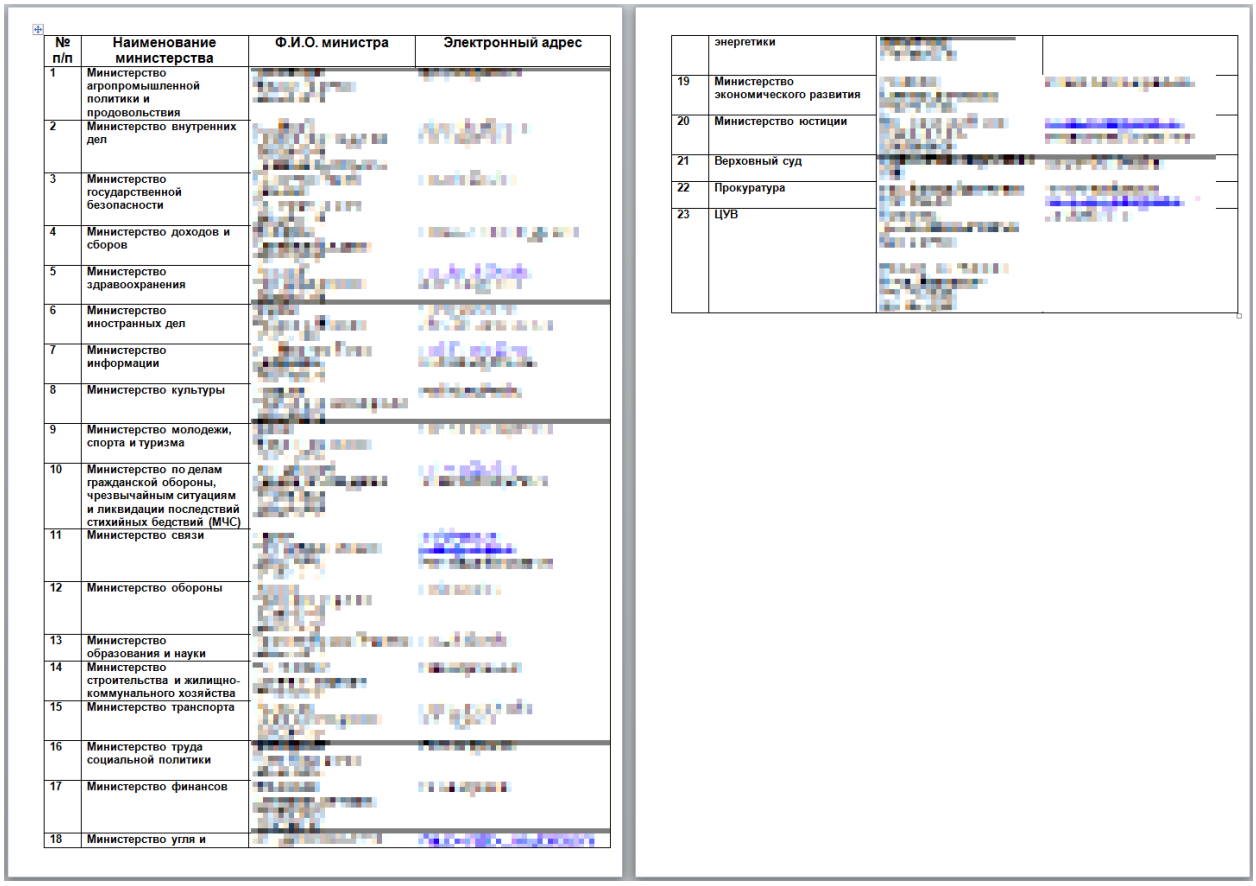
Велика кількість документів-приманок, використаних в атаках Prikormka, використовує теми стосовно самопроголошених Донецької та Луганської Народних Республік. Крім цього, ряд документів-приманок містить особисті дані, зокрема внутрішню статистику та документи, що, ймовірно, використовуються у внутрішньому документообігу самопроголошених республік. Це свідчить про те, що оператори програмного забезпечення навмисно атакували людей цих двох регіонів. Припущення підтвердили дані ESET LiveGrid®: найбільше жертв шкідливого програмного забезпечення Prikormka в Україні припадає на Донецьку та Луганську області.

Зловмисники використовують прийоми соціальної інженерії для переконання жертви відкрити шкідливе вкладення, серед яких використання провокативних та привабливих назв вкладень електронної пошти. Приклади таких назв:

- `Нацгвардейцы со шприцами сделали из донецкого мальчика мишень для ракет.exe`
- `Последнее обращение командира бригады 'Призрак' Мозгового Алексея Борисовича к солдатам и офицерам ДНР и ЛНР.scr`
- `Места дислокации ВСУ в зоне проведения АТО.scr`

Нижче наведені приклади документів-приманок, які були використані під час атак у Луганській та Донецькій областях.

Перший приклад — файл з назвою `СПРАВОЧНИК по МИНИСТЕРСТВАМ обновленный.exe`, що запускає документ-приманку з переліком міністерств самопроголошених республік. ID кампанії для цього файлу став `D_xxx`.



№ п/п	Наименование министерства	Ф.И.О. министра	Электронный адрес
1	Министерство агропромышленной политики и продовольствия		
2	Министерство внутренних дел		
3	Министерство государственной безопасности		
4	Министерство доходов и сборов		
5	Министерство здравоохранения		
6	Министерство иностранных дел		
7	Министерство информации		
8	Министерство культуры		
9	Министерство молодежи, спорта и туризма		
10	Министерство по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС)		
11	Министерство связи		
12	Министерство обороны		
13	Министерство образования и науки		
14	Министерство строительства и жилищно-коммунального хозяйства		
15	Министерство транспорта		
16	Министерство труда социальной политики		
17	Министерство финансов		
18	Министерство угля и		

	энергетики		
19	Министерство экономического развития		
20	Министерство юстиции		
21	Верховный суд		
22	Прокуратура		
23	ЦУВ		

Рис. 3. Документ-приманка зі списком міністерств ДНР
(тут і далі потенційно конфіденційні дані були відредаговані спеціалістами ESET)

Іншим прикладом документа-приманки є файл з назвою `материалы к зачету по законодательству.exe`. Цей файл запускав кілька документів, включаючи тимчасову конституцію ЛНР, а також інші правові та політичні документи. ID кампанії є `L_ment`. Використання у назві сленгового слова «мент» свідчить про вільне володіння зловмисниками російською мовою.

ЛУГАНСКАЯ НАРОДНАЯ РЕСПУБЛИКА

ЗАКОН

Об оперативно-розыскной деятельности

Настоящий Закон определяет содержание оперативно-розыскной деятельности, осуществляемой на территории Луганской Народной Республики, и закрепляет систему гарантий законности при проведении оперативно-розыскных мероприятий.

Глава I. Общие положения

Статья 1. Оперативно-розыскная деятельность

Оперативно-розыскная деятельность - вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим Законом (далее - органы, осуществляющие оперативно-розыскную деятельность), в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.

Статья 2. Задачи оперативно-розыскной деятельности

Задачами оперативно-розыскной деятельности являются:

Рис. 4. Документ-приманка із законом, який містить правила для спеціальних дій щодо розслідування злочинів

Деякі з документів-приманок використовують тему Мінських домовленостей. Прикладом такого документу є файл з назвою `Схема демилитаризованной зоны в районе Широкино.exe`. ID кампанії став `Lminfin`.

ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА

Рабочая группа по реализации
Комплекса мер по выполнению
Минских соглашений

DONETSK PEOPLE'S REPUBLIC

Working Grouponthe
implementation of set of measures
on the execution of Minsk Agreements

Исх. [redacted] от 04 июля 2015 г

[redacted]

копия:

[redacted]

Направляю в Ваш адрес схему демилитаризованной зоны в районе н.п. Широкино и отвода вооруженных формирований Донецкой Народной Республики в одностороннем порядке.

Полномочный представитель
Донецкой Народной Республики
на переговорах Контактной
группы в Минске

Д.В. Пушилин

ПОЛНОМОЧНЫЙ ПРЕДСТАВИТЕЛЬ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
НА ПЕРЕГОВОРАХ КОНТАКТНОЙ ГРУППЫ В МИНСКЕ

Рис. 5. Документ-приманка, який використовує тему Мінських домовленостей

Ще один подібний документ з назвою `Отвод с 4 участками по сост на 14.08.exe` навіть містить карту буферної зони, визначеною Мінським протоколом. ID кампанії – `BUR`.

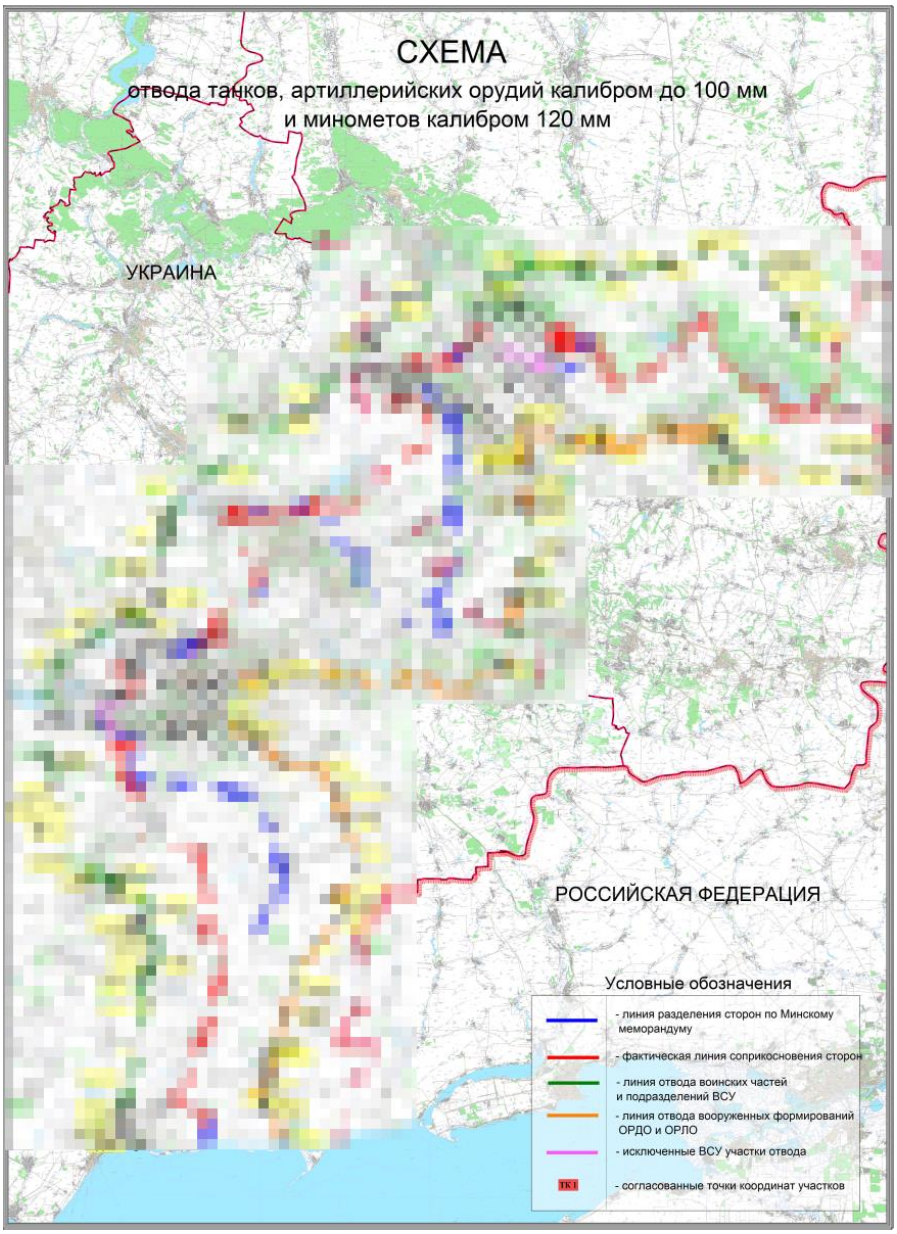


Рис. 6. Документ-приманка з картою буферної зони

Важливе зауваження: більшість бінарних файлів Prikormka, які використовуються для атаки на окупованих територіях, мають ID кампанії з початковими символами D або L. Цілком можливо, що це означає Донецька та Луганська Народні Республіки відповідно. Крім цього, також було виявлено файл з назвою `Заявление Эдуарда Басаргина 13 октября 2015 года в 15 часов.exe`, який використовує ID кампанії `RF_lgm`. Після виявлення в Росії даного файлу префікс RF може розшифровуватися як Російська Федерація.

Кампанії проти українських націоналістичних політичних партій

Усі попередні документи-приманки взяті з виконуваних файлів з російськими назвами. В Україні українська мова є офіційною державною мовою, але жителі Східної України, як правило, використовують російську мову, на відміну від західних регіонів, де розмовляють переважно українською мовою.

Однак деякі бінарні файли Prikormka мали українські назви. Раніше йшлося про файл з назвою `План ДНР на 21 липня, щодо відводу військ.exe`. Назви файлів українською мовою дозволяють зробити припущення, що одержувачі шкідливих листів спілкуються переважно українською мовою. Факт виявлення небезпечного програмного забезпечення Prikormka в західних областях України підтверджує це припущення.

ID кампанії для даного виконуваного файлу був `Psek`, який свідчить про те, що члени української націоналістичної партії Правий сектор теж були під прицілом кіберзлочинців.

ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА

Рабочая группа по реализации Комплекса мер по выполнению Минских соглашений

DONETSK PEOPLE'S REPUBLIC

Working Grouponthe implementation of set of measures on the execution of Minsk Agreements

Исх. от 20 июля 2015 г

Представителям СММ ОБСЕ в Донецкой Народной Республике

Сообщаем Вам, что руководством ДНР принято решение об одностороннем отводе вооружений калибром менее 100 мм и танков от линии соприкосновения сторон в соответствии с Минскими договоренностями.

21 июля 2015 г. В 11.00 (по мск) под контролем СММ ОБСЕ планируется отвести восемь единиц техники:

№ п/п	наименование вооружения	бортовой номер	номер корпуса/КПП (башня)
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

Полномочный представитель Донецкой Народной Республики на переговорах Контактной группы в Минске

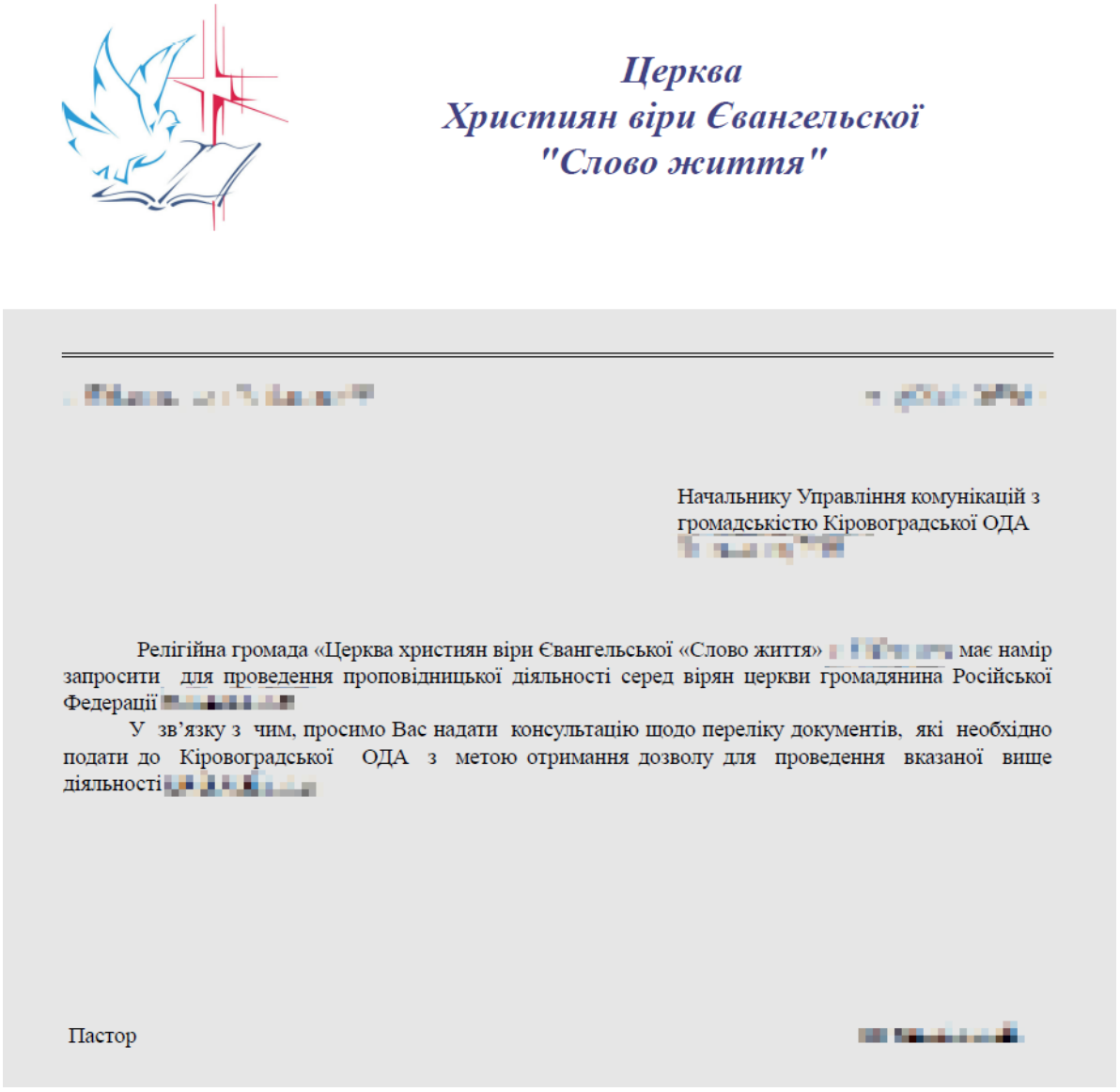
Д.В. Пушилин

Рис. 7. Документ-приманка, який, можливо, використовували проти членів української націоналістичної партії.

Інші кампанії

Жителі Донецької та Луганської областей, а також інші згадані жертви були не єдиними мішенями Операції Groundbait («Прикормка»). Спеціалісти ESET дослідили й інші кампанії з цікавими документами-приманками, однак на базі цих документів не вдалося встановити жертв кіберзлочинців.

Нижче поданий приклад документа-приманки, який можливо використали проти релігійних організацій. Документ-приманка був названий `Новое слово жизни.exe`. ID даної кампанії – `medium`, що може бути пов'язано з екзотерикою (медіумізмом) та спіритизмом.



Церква
Християн віри Євангельської
"Слово життя"

Начальнику Управління комунікацій з громадськістю Кіровоградської ОДА

Релігійна громада «Церква християн віри Євангельської «Слово життя» має намір запросити для проведення проповідницької діяльності серед вірян церкви громадянина Російської Федерації

У зв'язку з чим, просимо Вас надати консультацію щодо переліку документів, які необхідно подати до Кіровоградської ОДА з метою отримання дозволу для проведення вказаної вище діяльності

Пастор

Рис. 8. Документ-приманка, який, можливо, використовували проти релігійних організацій

Інша кампанія була виявлена в березні 2016 року. Цього разу шкідливий файл був підписаний угорською мовою: `Önéletrajz fizikai munka 2.pdf.scr`, що перекладається як «Резюме фізична праця». Документом-приманкою слугував файл з резюме угорською мовою. Цей шкідливий файл `.SCR` був відправлений єдиним архівом з двома іншим документами: резюме особи українською та сертифікат угорською мовами з підтвердженням здатності цієї людини виконувати фізичну роботу. Володіючи лише цією інформацією, важко встановити мішень кіберзлочинців. Однак факт необхідності знання одержувачем угорської та української мов підвищує інтерес до цієї кампанії. ID кампанії був `F_ego`.

Szám: Som/2013/1/23

TANÚSÍTVÁNY

[redacted]

[redacted] - Kabinet mint vizsgaszervező előtt az egyes rendészeti feladatokat ellátó személyek tevékenységéről, valamint egyes törvényeknek az iskolakerülés elleni fellépést biztosító módosításáról szóló 2012. évi CXX. törvény 23. §-ában meghatározottak alapján a személy- és vagyonőrök képzését követően ***megfelelt minősítéssel***

VIZSGÁT

tett.

Kelt: Kaposvár (7400), Somssich P. u. 15., MÁV Kollégium, 2013. év 06. hó 10. nap

P.H.

Vagyonvédelmi és Magánnyomozói Szakmai Kamara Országos Szervezete Somogy Megyei Szervezete

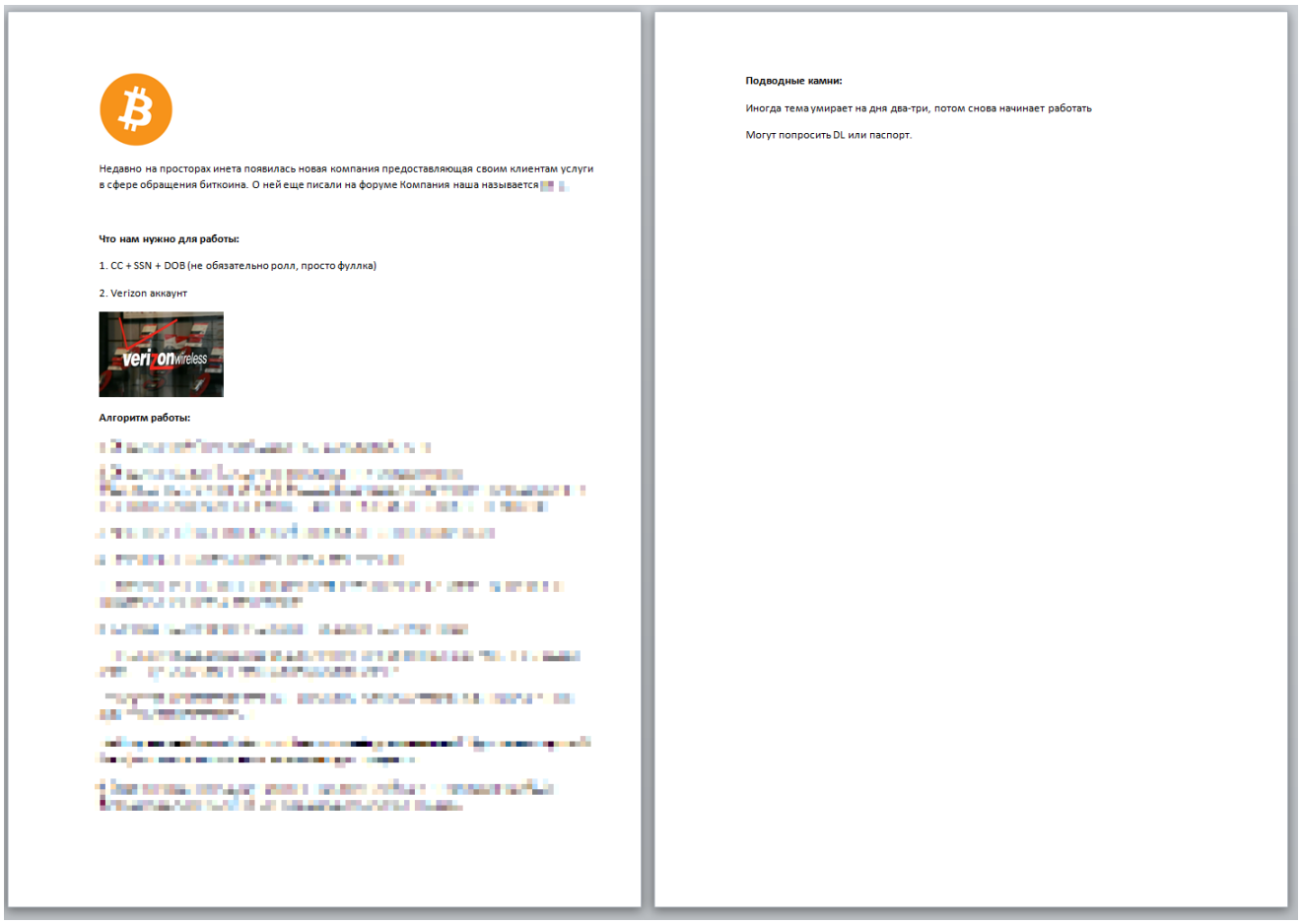
vizsgaszervező vezetője

vizsgabizottság elnöke

13

Рис. 9. Документ угорською мовою, який надсилали жертві в одному архіві зі шкідливою програмою Prikormka

Нижче наведено приклад документа-приманки, який надсилався файлом з назвою `bitcoin.exe`. ID кампанії в даному випадку був `hmod`.



Недавно на просторах инета появилась новая компания предоставляющая своим клиентам услуги в сфере обращения биткоина. О ней еще писали на форуме Компания наша называется

Что нам нужно для работы:

1. CC + SSN + DOB (не обязательно ролл, просто фуллка)

2. Verizon аккаунт

Алгоритм работы:

Подводные камни:

Иногда тема умирает на дня два-три, потом снова начинает работать

Могут попросить DL или паспорт.

Рис. 10. Документ-приманка, який пояснює механізм шахрайства з кредитними картками

Текст російською мовою в документі-приманці покроково пояснює, як купити віртуальну валюту Bitcoin, використовуючи вкрадені кредитні картки. Текст рясніє сленговими словами, що часто використовуються російськомовними кардерами.[1]

[1] Кіберзлочинці, які здійснюють операції із вкраденими кредитними картками.

Іншим прикладом є загадковий документ-приманка, вилучений зі шкідливої програми, з назвою `prikormka.exe`. ID кампанії став `30K_alfa`.

Официальный представитель "FIN" в Украине

[redacted]

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 $

Рис. 11. Загадковий документ-приманка, витягнутий з файлу `prikormka.exe`.

Цей документ-приманка містить прейскурант українського магазину, який продає різні види прикормки для риб.

Технічні деталі

У цій частині подано опис технічних аспектів загрози Prikormka, включно з архітектурою шкідливого програмного забезпечення, зв’язком з командним сервером та детальним аналізом використаних модулів.

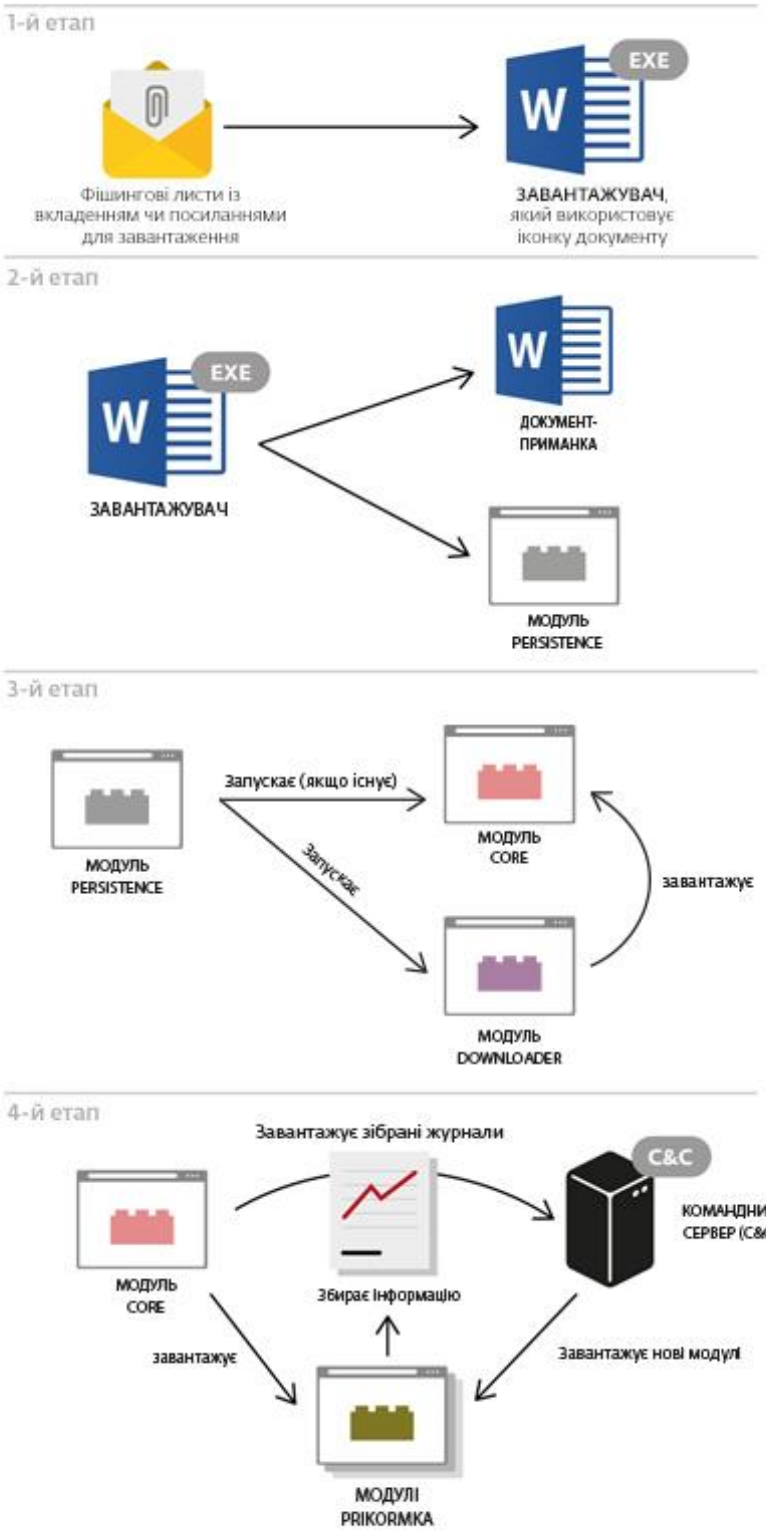


Рис. 12. Спрощена схема архітектури шкідливого програмного забезпечення Prikormka.

Завантажувач

Завантажувач є початковим компонентом шкідливої програми Prikormka, яка, як правило, поширюється через вкладення електронної пошти. Зазвичай, завантажувач з розширенням файлу `.SCR` або `.EXE` міститься в архіві. З метою введення в оману жертви завантажувач Prikormka може поширюватися під виглядом різних типів документів або архіву ізздатністю до саморозпаковування.

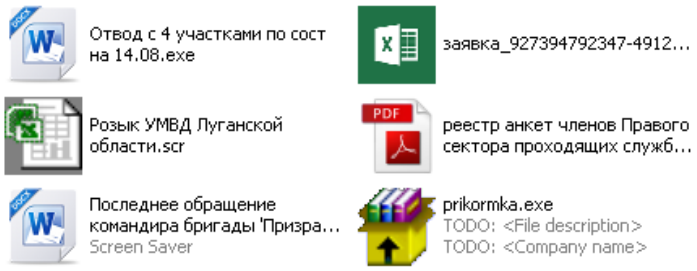


Рис. 13. Іконки, які використовуються шкідливою програмою Prikormka.

Відкриваючи один або кілька документів-приманок, завантажувач інфікує комп'ютер. Для цього шкідлива програма відображає вікно архіву WinRAR із здатністю до саморозпаковування (SFX). У деяких випадках завантажувач створює легітимний, не шкідливий виконуваний файл SFX на диску, а потім запускає його. Архів SFX завжди має російський графічний інтерфейс користувача, навіть у випадках назви завантажувача українською мовою. Завантажувач з угорською назвою файлу не відображає дане вікно взагалі.

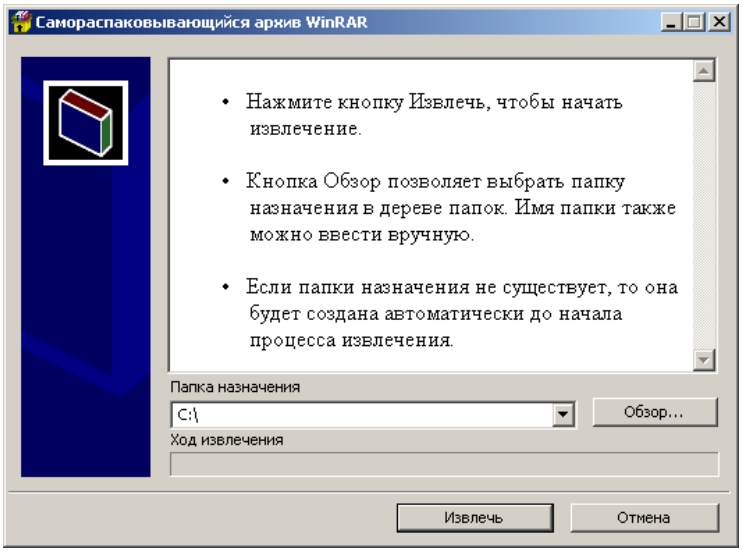


Рис. 14. Російський інтерфейс архіву SFX.

Виконуваний файл SFX може містити один або кілька документів-приманок. Наприклад, один з SFX файлів загрози міститься 24 документа. Звичайно, кількість та розмір документів-приманок впливає на розмір завантажувача. Найбільший завантажувач, який був знайдений спеціалістами ESET, мав розмір файлу 25 Мб.

Більшість завантажувачів мають вбудований маніфест додатку, який вимагає права адміністратора виконуваного файлу для запуску системи. У разі відсутності у користувача прав адміністратора система буде запитувати дані облікового запису.

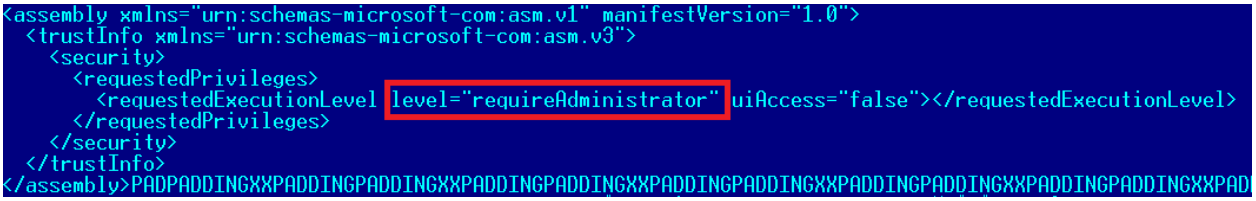


Рис. 15. Вбудований маніфест додатку, розміщений у завантажувачі Prikormka

Вимога наявності права адміністратора для завантажувача допомагає кіберзлочинцям зробити інфікування системи більш стійким. Зокрема шкідлива програма використовує так званий DLL порядок завантаження для автоматичного запуску загрози під час кожного завантаження системи. Завантажувач зберігає один з модулів DLL Prikormka в директорії Windows з назвою `ntshrui.dll`. Оскільки цей файл зберігається в директорії Windows, під час запуску системи він завантажується як процес `explorer.exe` замість легітимного файлу ntshrui.dll, який зберігається в підкаталозі `C:\Windows\System32`. Таким чином, модуль Prikormka несанкціоновано змінює порядок завантаження DLL-файлів. Цей метод не є новим, раніше він кілька разів був публічно розглянутий виробниками антивірусного програмного забезпечення.

Шкідливе програмне забезпечення Prikormka застосовує ще один цікавий метод з використанням файлових розширень `.SCR`, які підтримують екранну заставку та є стандартними виконуваними файлами Windows. Основною відмінністю між `.EXE` та `.SCR` є те, що екранна заставка виконується за допомогою функції спеціального командного рядка. Зазвичай, кіберзлочинці просто перейменовують розширення для уникнення заходів безпеки на основі розширень. Крім цього, автори шкідливого програмного забезпечення застосовують перевірку для даної функції командного рядка. У разі запуску бінарного файлу у вигляді стандартного файлу (без необхідних функцій) він не буде інфікувати систему. Таким чином, ця проста перевірка дозволила шкідливому програмному забезпеченню обійти деякі механізми захисту, які використовуються для автоматичної обробки зразків.

У випадках поширення загрози через файл `.SCR`, троянська програми використовує стандартні методи для завантаження DLL через `rundll32.exe` та підтримує стійкість, встановивши запис з назвою `guidVGA` або `guidVSA` в ключі реєстру запуску:

```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run]
```

Для завантаження 32-бітною та 64-бітною версією Windows Explorer шкідлива програма має виконувані файли для обох версій. Більшість модулів написано на мові програмування C і скомпільовані за допомогою Microsoft Visual Studio.

Завантажувач зберігає модулі в своїх ресурсах; деякі з цих ресурсів зашифровані за допомогою простої операції XOR.

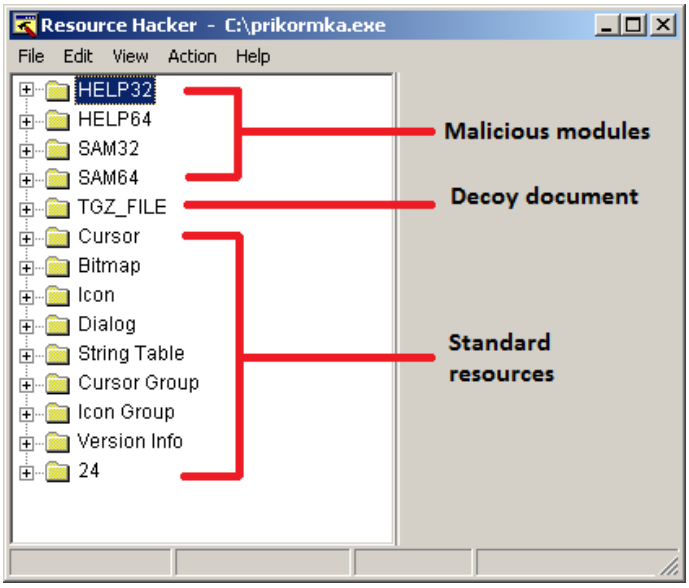


Рис. 16. Ресурси, розташовані всередині завантажувача бінарних файлів Prikormka

Завантажувач відповідає за створення файлу `rbcon.ini`, який шкідлива програма використовує для зберігання ID кампанії та інших значень.

Попередні версії Prikormka використовували інший метод — ID кампаній були вбудовані в бінарний файл одного з модулів:

```
.1001903C:  2F 01 00 00-4D 01 00 00-6C 01 00 00-77 00 77 00  /☺  M☺  l☺  w w
.1001904C:  77 00 2E 00-67 00 69 00-6C 00 73 00-2E 00 68 00  w . g i l s . h
.1001905C:  6F 00 2E 00-75 00 61 00-00 00 00 00-6C 00 70 00  o . u a     l p
.1001906C:  6C 00 00 00-6B 00 70 00-6C 00 00 00-69 00 70 00  l   k p l   i p
.1001907C:  6C 00 00 00-6D 00 6D 00-74 00 6D 00-70 00 00 00  l   m m t m p
.1001908C:  68 00 6D 00-79 00 72 00-33 00 32 00-00 00 00 00  h m y r 3 2
.1001909C:  70 00 6C 00-2E 00 70 00-68 00 70 00-00 00 00 00  p l . p h p
.100190AC:  5C 00 00 00-2F 00 00 00-68 00 74 00-74 00 70 00  \   /   h t t p
.100190BC:  3A 00 2F 00-2F 00 00 00-73 00 65 00-00 00 00 00  : / /   s e
.100190CC:  69 00 65 00-72 00 64 00-69 00 72 00-2E 00 64 00  i e r d i r . d
.100190DC:  61 00 74 00-00 00 00 00-5B 45 6E 64-50 6F 69 6E  a t     [EndPoin
.100190EC:  74 5D 00 00-D4 5C 01 10-6C 5E 01 10-64 5E 01 10  t]  ╘\☺►l^☺►d^☺►
```

Рис. 17. ID кампанії зі значенням hmyr32, який вбудований в бінарний файл

Значення ID кампанії було жорстко закодовано в бінарний файл Prikormka під час компіляції. Крім цього, ID в 32-бітній версії бінарних файлів закінчувався на 2. У той же час ID кампанії в 64-бітній версії бінарних файлів закінчувався на 4.

Цей метод був ефективний з невеликою кількістю жертв, однак зі зростанням кількості інфікованих пристроїв кіберзлочинці зіштовхнулися з рядом проблем. Цілком ймовірно, що перекомпіляція та перепакування основних частин набору інструментів для кожної нової жертви займали багато часу. Тож в середині 2015 року зловмисники змінили дану схему. З червня 2015 року ID кампанії зберігається в окремому файлі з назвою `rbcon.ini`, який зловмисники називають `objectset`. До шкідливої програми автори також включили нове значення `roboconid`, який є ID оператора. Дослідження ESET підтвердило, що даний ідентифікатор є унікальним номером оператора шкідливої програми, який здійснює кібероперації для інфікування, шпигування та відслідковування з певною метою.

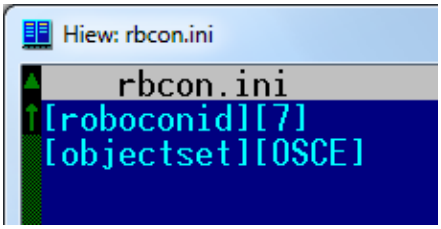


Рис. 18. Файл `rbcon.ini`, який містить ID кампанії та ID оператора

Деякі з бінарних файлів завантажувача містять PDB-шлях, який може розкрити структуру директорії, яка використовувалася зловмисниками.

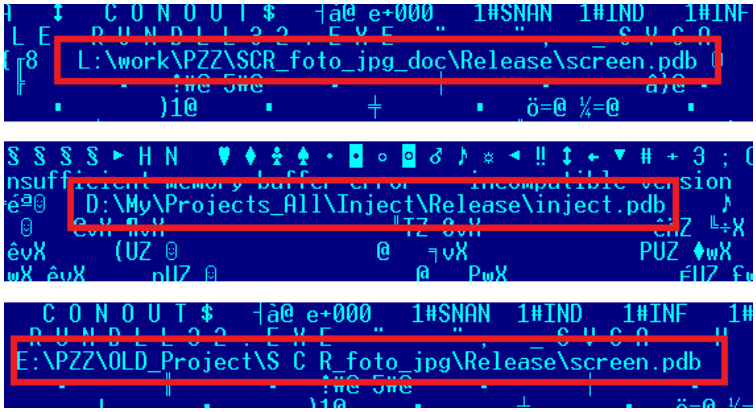


Рис. 19. Деякі з PDB-шляхів, виявлених всередині завантажувачів Prikormka

Автори шкідливих програм називають шкідливу програму Trojan PZZ, спеціалісти ESET мають інші докази цієї теорії.

Сімейство Prikormka є типовою троянською програмою-кібершпигуном з модульною архітектурою. Функціональність троянської програми дозволяє зловмисникам викрадати конфіденційні дані з інфікованого пристрою та завантажувати їх на командні сервери (C&C).

Модулі Prikormka

Модулі Prikormka зберігаються на диску в інфікованій системі у вигляді DLL-файлів. Серед них — модулі для різних цілей, наприклад, для зв'язку з командним сервером, допоміжних цілей (наприклад, стійкість) та ексфільтрації різних видів конфіденційної інформації з інфікованого комп'ютера. Як згадувалося раніше, модулі Prikormka створені для 32-бітної та 64-бітної версій Windows.

Існує стандартний набір модулів для завантаження із заздалегідь визначеними назвами, які будуть детально описані в наступних частинах. Для виконання модуль (DLL-файл) має зберігатися з певним ім'ям файлу на диску та повинен мати одну з функцій експорту: `Starting`, `KickInPoint`, `Cycle`. Проте зловмисники можуть використати будь-який модуль користувача для конкретної жертви. Також спеціалісти ESET виявили, що призначені для користувача модулі зловмисники, зазвичай, називають `mp.dll`.

Слід зазначити, що оператори шкідливого програмного забезпечення приймають рішення про використання певних модулів для інфікування комп'ютера.

Prikormka може зберігати модулі з різною функціональністю зі схожими назвами або навпаки зберігати модулі з аналогічною функціональністю з різними назвами. Деякі версії шкідливого програмного забезпечення зберігають модулі з назвою файлу, який містить тільки поточну дату та час. У зв'язку з цим спеціалісти ESET назвали плагіни відповідно до назв кодів, які подані нижче.

Ім'я модульного коду	Внутрішнє ім'я модулю	Ім'я файлу	Мета
PERSISTENCE	samlib.dll	samlib.dll, ntshrui.dll	Використовується для довготривалого зберігання
DOWNLOADER	helpldr.dll	helpldr.dll, _wshdmi.dll	Модуль завантаження CORE
CORE	hauthuid.dll	hauthuid.dll, _svga.dll, _wshdmi.dll	Завантажує всі інші модулі, обмінюється даними з C&C-серверів,завантажує журнали
DOCS_STEALER	iomus.dll	iomus.dll	Збиріє документи
KEYLOGGER	kl.dll, hlpuctf.dll	hlpuctf.dll	Створює журнали натискань клавіш
SCREENSHOTS	scrsh.dll	scrsh.dll	Збирає скріншоти робочого столу
MICROPHONE	snm.dll	snm.dll	Фіксує звук з мікрофона
SKYPE	swma.dll	swma.dll	Записує аудіо дзвінки Skype
LOGS_ENCRYPTER	atiml.dll	atiml.dll	Стискає та шифрує зібрані журнали
GEOLOCATION	geo.exe	Inv.exe	Визначає географічне положення інфікованого комп'ютера
OS_INFO	InfoOS	mp.dll	Збирає інформацію про інфікований комп'ютер
PASSWORDS	Brother	mp.dll	Збирає збережені паролі для різних програм
FILE_TREE	mpTREE	mp.dll	Збирає файлове дерево з фіксованого диску з інфікованого комп'ютера

Таблиця 1. Список модулів Prikormka, виявлених спеціалістами ESET в ході дослідження.

Поданий список містить назви файлів модулів, виявлених в межах шкідливого коду, однак спеціалісти ESET не зіштовхувалися з ними в ході дослідження та відповідно не могли оцінити їх функціональні можливості:

- `miron.dll`
- `meta.dll`
- `hmuid.dll`
- `sh.exe`
- `mupdate.exe`

Важливо відзначити, що компоненти Prikormka, зроблені раніше (період між 2008 та 2010 роками) використовували зовсім іншу схему найменувань. Ось деякі приклади назв такий файлів:

- `smdhostn.dll`
- `heading.dll`
- `lgs.dll`
- `la.dll`
- `lh.exe`
- `lp.exe`
- `inl.exe`
- `lid.dll`

Модуль PERSISTENCE

Як зазначалось раніше, даний модуль використовує метод DLL порядку завантаження для підтримки стійкості системи.

Під час запуску цей модуль створює папку `%USERPROFILE%\AppData\Local\MMC` та копіює в неї такі файли з каталогу `%WINDIR%`:

- `hauthuid.dll (CORE)`
- `hlpuctf.dll (KEYLOGGER)`
- `atiml.dll (LOGS_ENCRYPTER)`
- `iomus.dll (DOCS_STEALER)`
- `swma.dll (SKYPE)`
- `helpldr.dll (DOWNLOADER)`
- `rbcon.ini`

Цей компонент згодом завантажує та передає виконання до модулю CORE, або до модулю DOWNLOADER, якщо не знайдено модуль CORE.

У разі наявності файлу `%USERPROFILE%\AppData\Local\MMC\nullstate.cfg` компонент видаляє всі назви файлів, перераховані вище, з каталогу `MMC` і завершує роботу, таким чином дезактивуючи себе.

Деякі з бінарних файлів модуля PERSISTENCE містять PDB-шлях, який розкриває структуру каталогів, яка використовувалася авторами шкідливого програмного забезпечення під час компіляції. Три з цих шляхів містять мітку часу, ймовірно, моменту створення або зміни проекту. Один такий шлях містить рядок російською мовою `Раб.программы`.

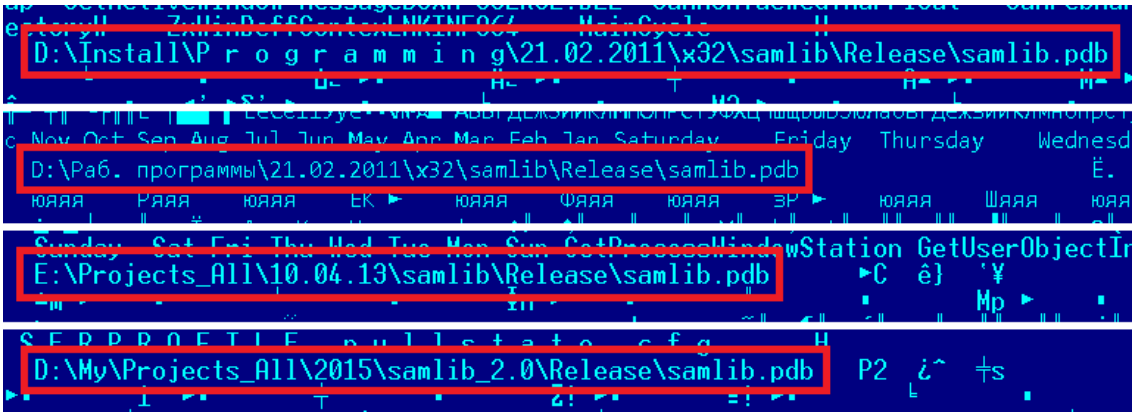


Рис. 20. Деякі з PDB-шляхів, виявлених всередині модуля PERSISTENCE Prikormka.

Модуль DOWNLOADER

Основною метою даного компонента є завантаження модуля CORE та його виконання.

Модуль DOWNLOADER подає HTTP запит до одного зі своїх командних серверів, отримує та розшифровує дані, зберігає їх під назвою `hauthuid.dll`, а потім завантажує DLL. Зв'язок шифрується за допомогою шифру Blowfish, а потім кодується base64.

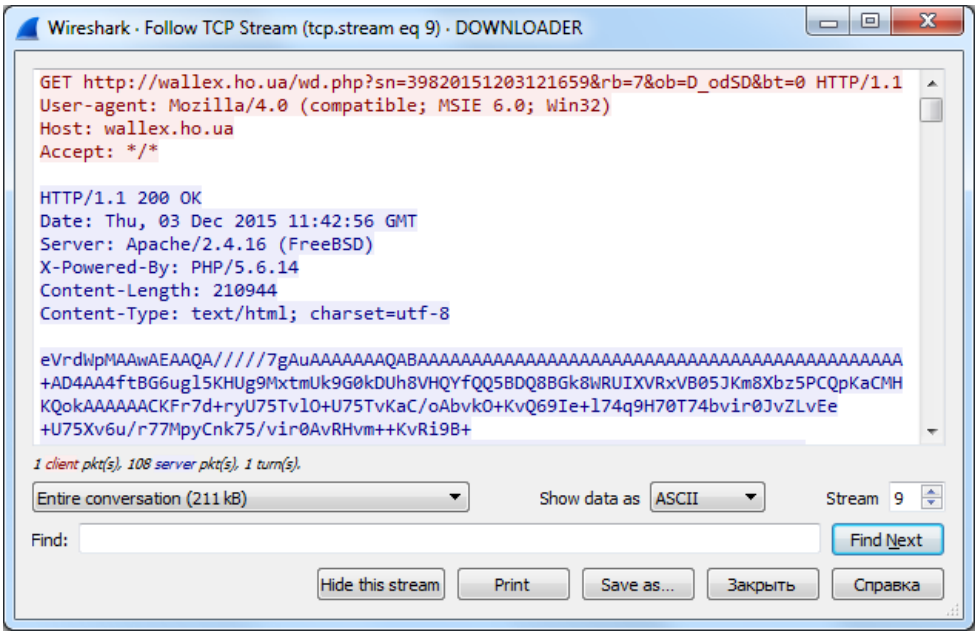


Рис. 21. Трафік модуля DOWNLOADER шкідливого програмного забезпечення Prikormka

Окрім ID кампанії та ID оператора, модуль включає в запит дату та час інфікування, а також 32-бітну або 64-бітну версію Windows.

Деякі з бінарних файлів модуля DOWNLOADER містять PDB-шлях, показуючи, що всередині цей модуль має назву `Loader` чи `helpldr`:

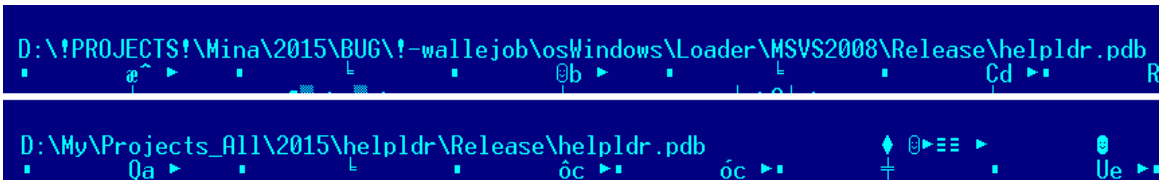


Рис. 22. PDB-шлях, виявлений всередині модуля DOWNLOADER.

Модуль CORE

Модуль CORE відповідає за зв'язок з командними серверами та інші завдання, включаючи завантаження додаткових модулів та відправлення вкрадених даних на віддалений сервер.

З часу появи шкідливого програмного забезпечення (і модулю CORE зокрема), деталі його реалізації варіювалися, але основна концепція модуля CORE залишалася незмінною протягом багатьох років. Концепція шкідливої програми Prikormka проста: модуль CORE завантажує додаткові компоненти, які використовуються для збору різних типів даних. Після завантаження компонент збирає конфіденційну інформацію та зберігає цю інформацію в певний системний журнал, який може зберігати зібрані дані в

форматі простого тексту або зашифровувати інформацію. Модуль CORE періодично перевіряє такі системні журнали і у разі їх доступності він буде завантажувати журнал на віддалений сервер. Модуль CORE не зможе завантажити системний журнал розміром понад 500 Мб.

Для того, щоб зберегти завантажені модулі та зібрати системні журнали, модуль CORE створює дві директорії:

- `%USERPROFILE%\AppData\Local\MMC\`
- `%USERPROFILE%\AppData\Local\SKC\`

Папка MMC переважно використовується для завантаження додаткових шкідливих компонентів; папка SKC потрібна для зберігання зібраних системних журналів. Надалі термін «папка журналу» буде використовуватися для позначення директорії SKC.

Завантажені модулі не здатні завантажити зібрані дані. Насправді, тільки модулі CORE та DOWNLOADER обмінюються даними з командним сервером, а протокол зв'язку модуля CORE дуже подібний до DOWNLOADER.

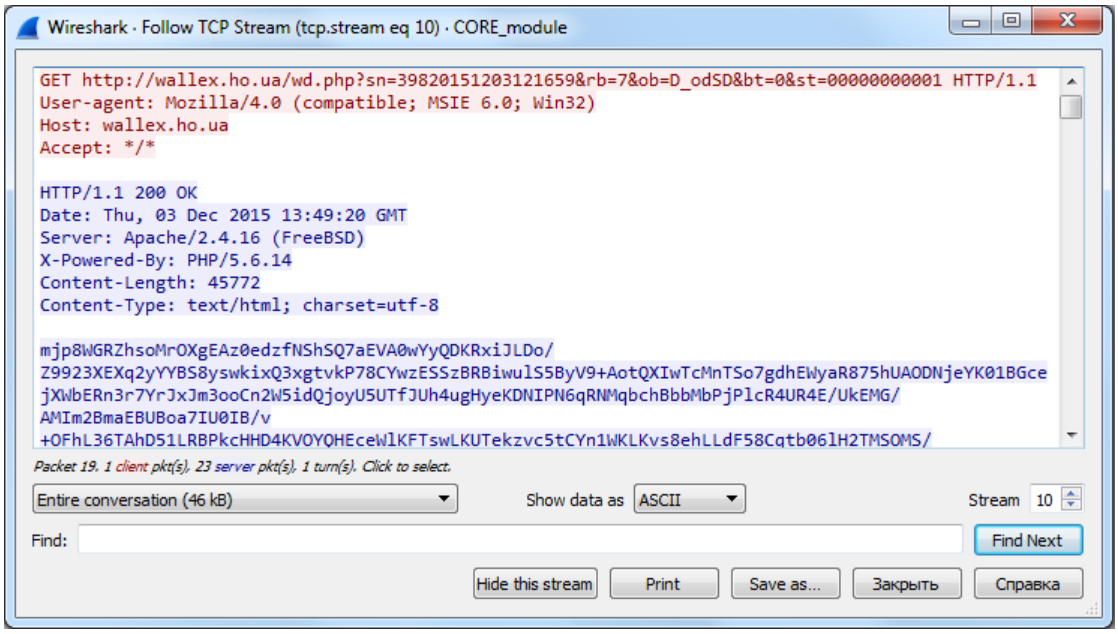


Рис. 23. Трафік модуля CORE шкідливого програмного забезпечення Prikormka

Єдиною відмінністю між запитами DOWNLOADER та CORE HTTP є `st` параметр в URL. Цей параметр вказує на те, які з завантажених модулів активні та завантажені загрозою Prikormka. З поточною реалізацією залишається місце для 11 додаткових модулів. Сервер застосовує у відповідь вміст модуля, який повинен бути виконаний, або фіктивну відповідь.

Журнали завантажуються під час запиту POST на подібний URL:

- `hxxp:/server.ua/wd.php?sn=%DATE_TIME_OF_INFECTION%`

Варто відзначити, що попередні версії Prikormka зберігали командні сервери в форматі простого тексту; пізніше зловмисники використовували алгоритм base64 для приховування адрес серверів. А останні версії основних модулів використовують просте шифрування: для його розшифрування необхідно додати шістнадцяткове значення 0x17 для кожного зашифрованого байта.

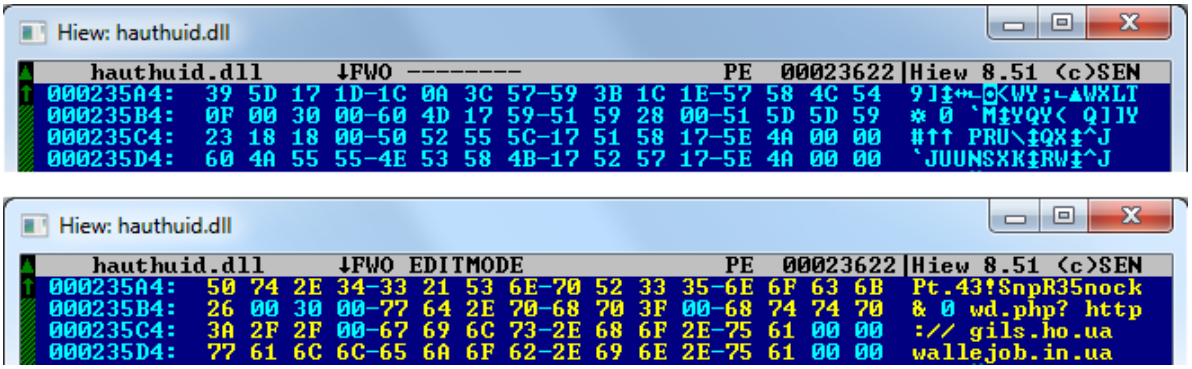


Рис. 24. Приклад простого шифрування, який використовує Prikormka для приховування командних серверів

Модуль DOCS_STEALER

Цей модуль відповідає за збір документів зі змінних носіїв або фіксованих дисків, підключених через інтерфейс USB.

Модуль фокусується на отриманні файлів з розширеннями документів типу: . DOC, .XLS, .DOCX, .XLSX, .PPT, .PPTX, .PPS, .PPSX, .PDF, .RTF, .TXT, .ODT. Проте він не збирає всі файли, а тільки ті, які були змінені протягом останніх 7 днів (або 14, або 30 залежно від версії модуля).

Зібрані файли потім стискаються, шифруються за допомогою Blowfish і зберігаються за такою схемою:

- `%USERPROFILE%\AppData\Local\ioctl\%DISK_ID%\%DATE%_%TIME%.kf`

Модуль KEYLOGGER

Цей модуль відповідає за збір комбінацій клавіш і назв переднього плану вікна.

Зібрана інформація зберігається в папці журналу з назвами:

- `%DATE%_%TIME%_fix.lg`
- `lgfix`
- `lpl`
- `fplid`
- `fmmlg`

У разі перевищення системним журналом обсягу 10 Мб модуль видаляє журнал і починає заново. Деякі версії модуля шифрують системні журнали за допомогою Blowfish.

Модуль SCREENSHOTS

Цей модуль відповідає за захоплення знімків екрану робочого столу жертви.

За замовчуванням модуль фіксує знімки екрану кожні 15 хвилин. Проте, якщо жертва відкриває VoIP додатки Skype або Viber, період між знімками різко зменшується до 5 секунд. Знімки екрану зберігаються в форматі JPEG.

Зібрана інформація розташовується в папці журналу з назвою `%DATE%_%TIME%.tgz.scrsh` або `%DATE%_%TIME%.stgz`.

Модуль MICROPHONE

Цей модуль відповідає за запис звуку мікрофону.

Модуль записує аудіо тривалістю 10 хвилин. Він припиняє запис за командою або у разі відсутності вільного місця на диску. Записаний звук кодується за допомогою кодувальника LAME MP3.

Зібрана інформація зберігається в папці журналу з назвою `%DATE%_%TIME%.snm`.

Модуль SKYPE

Модуль відповідає за запис аудіорозмов у Skype.

Для запису дзвінків Skype модуль використовує легітимний інтерфейс – Skype Desktop API. Коли сторонній додаток збирається використовувати цей API, Skype відображає користувачу попередження з запитом дозволити доступ. Щоб обійти функцію захисту Skype, модуль Prikormka створює потік повідомлень для знайдення вікна та натиснення кнопки «Дозволити доступ» програмним шляхом без залучення користувача.

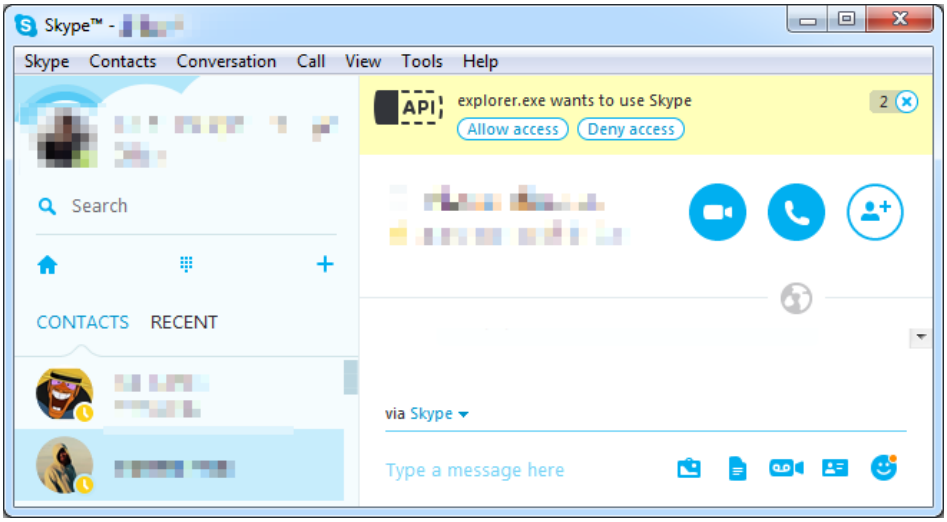


Рис. 25. Попередження, що відображається у Skype

Рядки і деякі фрагменти коду в цьому модулі загрози Prikormka дають зрозуміти, що його реалізація була частково запозичена з коду, опублікованого на сайті openrce.org у 2006 році.

```
.data:1001D0EC ; char str_MINISHELL[]
.data:1001D0EC str_MINISHELL   db 'CREATE APPLICATION minishell',0
.data:1001D0EC                                         ; DATA XREF: ProcessMessage+67↑o
.data:1001D0EC                                         ; SkypeAPI_Windows_WindowProc+3F↑o
.data:1001D109                 align 4
.data:1001D10C ; char str_CALL[]
.data:1001D10C str_CALL        db 'CALL %d',0          ; DATA XREF: get_CALL_ID+C↑o
.data:1001D114 ; char str_ALTER_CALL[]
.data:1001D114 str_ALTER_CALL  db 'ALTER CALL %d',0    ; DATA XREF: get_CALL_ID+26↑o
.data:1001D122                 align 4
.data:1001D124 ; char str_GET_CALL[]
.data:1001D124 str_GET_CALL    db 'GET CALL %d PARTNER_DISPNAME',0
.data:1001D124                                         ; DATA XREF: ProcessMessage+161↑o
```

Рис. 26. Рядок `CREATE APPLICATION minishell` пропонує скопіювати та вставити код.

Зібрана інформація зберігається в папці журналу, використовуючи назви файлів `%DATE%_%TIME%.skw` та `_skype.log`.

Модуль LOGS_ENCRYPTER

Цей модуль відповідає за шифрування журналу.

Модуль забезпечує стиснення даних за допомогою алгоритму LZSS та шифрує такі системні файли за допомогою Blowfish:

- `%USERPROFILE%\AppData\Local\MMC\inf`
- `%USERPROFILE%\AppData\Local\MMC\fsh`
- `%USERPROFILE%\AppData\Local\SKC\*.scrsh`
- `%USERPROFILE%\AppData\Local\SKC\*.snm`
- `%USERPROFILE%\AppData\Local\SKC\*.skw`
- Файли перераховані в `%USERPROFILE%\AppData\Local\MMC\ierdir.dat`

Файл `ierdir.dat` створюється модулем CORE. Він містить зашифрований список файлів, потрібних злочинцям для завантаження комп'ютера жертви.

Після шифрування оригінальні (не зашифровані) файли будуть видалені. Результати шифрування зберігаються в наступних файлах:

- `%USERPROFILE%\AppData\Local\MMC\ipl`
- `%USERPROFILE%\AppData\Local\MMC\kpl`

Зашифрований вміст додатково кодується за допомогою алгоритму base64. Перед початком модуль ставить там додатковий підпис:

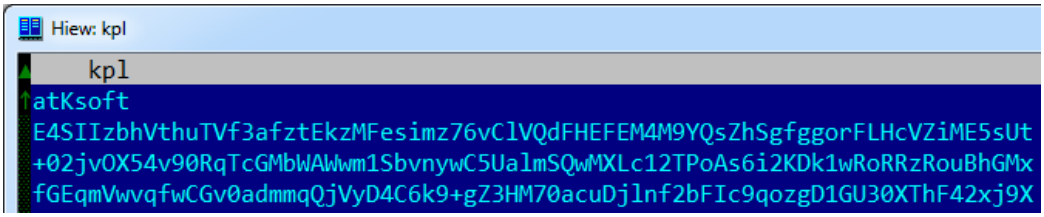


Рис. 27. Підпис "atKsoft" на початку зашифрованих системних файлів

Спеціалісти ESET не знайшли жодного легітимного додатку, який може читати такі файли або будь-які інші значення загадкового підпису "atKsoft".

Модуль GEOLOCATION

Цей модуль відповідає за геолокацію інфікованого комп'ютера.

На відміну від інших модулів, цей модуль написаний на мові програмування C#. Він збирає інформацію про доступні в даний час Wi-Fi мережі, включаючи Service Set Identifier (SSID) та MAC-адресу. Після цього модуль робить запит до сервісу Google, надаючи зібрану інформацію у вигляді параметрів; відповідь служби Google містить можливе місце розташування на основі наданої інформації.

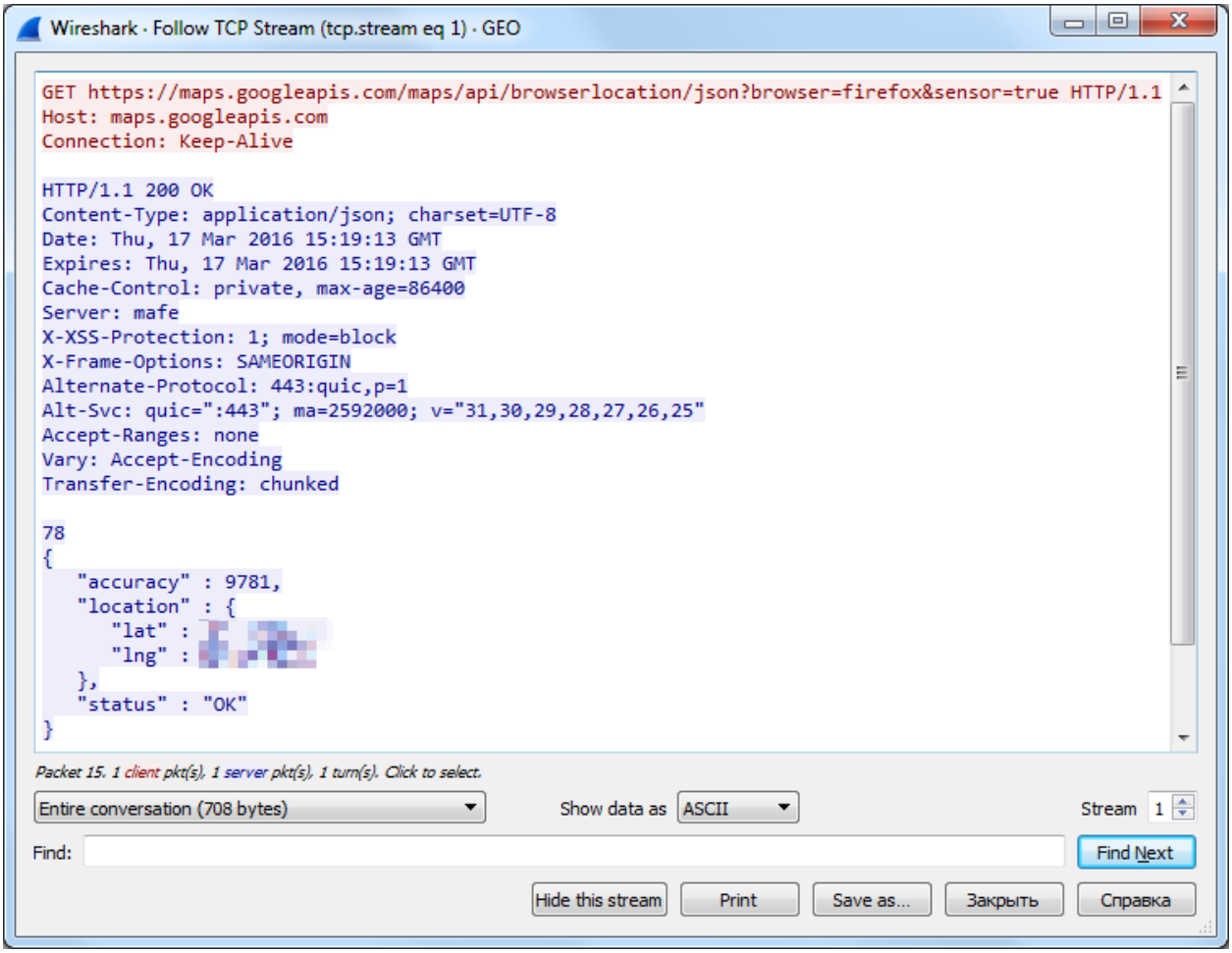


Рис. 28. Трафік захопленого загрозою Prikormka модуля GEOLOCATION

Зібрана інформація зберігається в папці журналу з назвою файлу `geo%DATE%.inf`.

Бінарний код модуля GEOLOCATION має PDB-шлях; структура цього шляху схожа на PDB-шлях модуля DOWNLOADER:

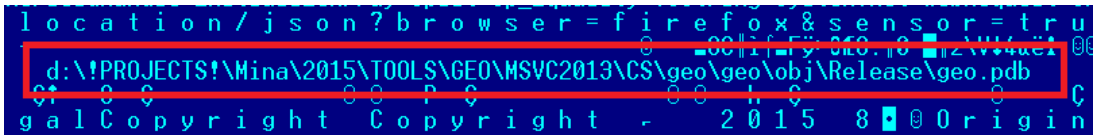


Рис. 29. PDB-шлях, виявлений всередині модуля GEOLOCATION

Модуль OS_INFO

Модуль відповідає за збір інформації про інфікований комп'ютер.

Даний модуль збирає таку інформацію:

- Інформація про батарею для ноутбуків
- Версія операційної системи Windows
- Ім'я комп'ютера та користувача
- IP-адреси та MAC-адреси
- Фізична пам'ять

- Доступні диски
- Доступні принтери
- Роздільна здатність екрану
- Встановлене антивірусне програмне забезпечення

Модуль використовує функції Windows API для збору цієї інформації.

Зібрана інформація зберігається в папці журналу під назвою `%DATE%_%TIME%.inf`.

Модуль PASSWORDS

Цей модуль відповідає за збір паролів, які зберігаються в браузерах, встановлених на інфікованому комп'ютері.

Модуль збирає версію програми, логіни та паролі, збережені в наступних браузерах:

- Google Chrome
- Opera Browser
- Yandex Browser
- Comodo Dragon Internet Browser
- Rambler Browser (Nichrome)
- Mozilla Firefox
- Mozilla Thunderbird

З певних причин цей модуль не збирає паролі для браузерів Microsoft Internet Explorer та Microsoft Edge. Оскільки браузери Yandex та Rambler користуються популярністю в основному в російськомовних країнах, спеціалісти ESET вважають, що даний модуль був розроблений для використання щодо користувачів таких країн.

Зібрана інформація зберігається в папці журналу з назвою `%DATE%_%TIME%.inf`.

Модуль FILE_TREE

Цей модуль відповідає за збір інформації про файлову систему фіксованих дисків комп'ютера, включаючи трафік файлів з певними розширеннями, їх розмір і час створення. Фактичний зміст файлу не береться до уваги цим модулем.

Кіберзлочинців цікавлять наступні розширення файлів:

- Документи: TXT, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF
- Архіви: ZIP, RAR
- Бази даних: DB, SQLITE
- Поштові клієнти The Bat!: TBB, CFG, CFN, TBN, TBB
- Microsoft Outlook: OST, PST
- Інші: DAT, WAV, EXE

Іншим свідченням того, що шкідливе програмне забезпечення створюється з наміром атакувати російськомовних користувачів, є популярність поштового сервісу The Bat! в російськомовних країнах.

Слід зазначити, що список всіх розширень файлів не є універсальним списком для кожного конкретного зразка. Цей список містить усі можливі розширення файлів, виявлені спеціалістами ESET в різних версіях модуль FILE_TREE. Тоді як кіберзлочинці могли створити власну версію цього модуля для конкретної жертви.

Зібрана інформація зберігається в папці журналу під назвою `%DATE%_%TIME%_tree.inf`.

Деякі бінарні файли модулів FILE_TREE мають PDB-шлях; один такий шлях показує ім'я користувача автора шкідливої програми.

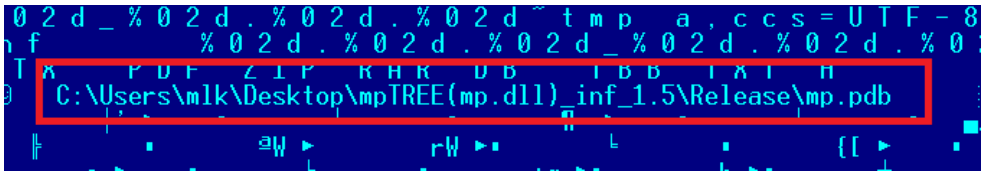


Рис. 30. PDB-шлях, виявлений всередині модуля FILE_TREE

Командні сервери (C&C)

У ході дослідження операції Groundbait спеціалісти ESET виявили ряд доменів командних серверів та IP-адрес. Більшість з них розташовані в Україні та розміщені українськими хостинг-провайдерами. Додаток 2 містить повний перелік цих доменів та IP-адрес.

Один з командних серверів `gils.ho[.]ua` використовується в операції з 2008 року, відповідно до інформації, отриманої від хостинг-компанії. Для прикриття своєї незаконної діяльності, зловмисники створили підробний веб-сайт, присвячений столиці України — Києву.

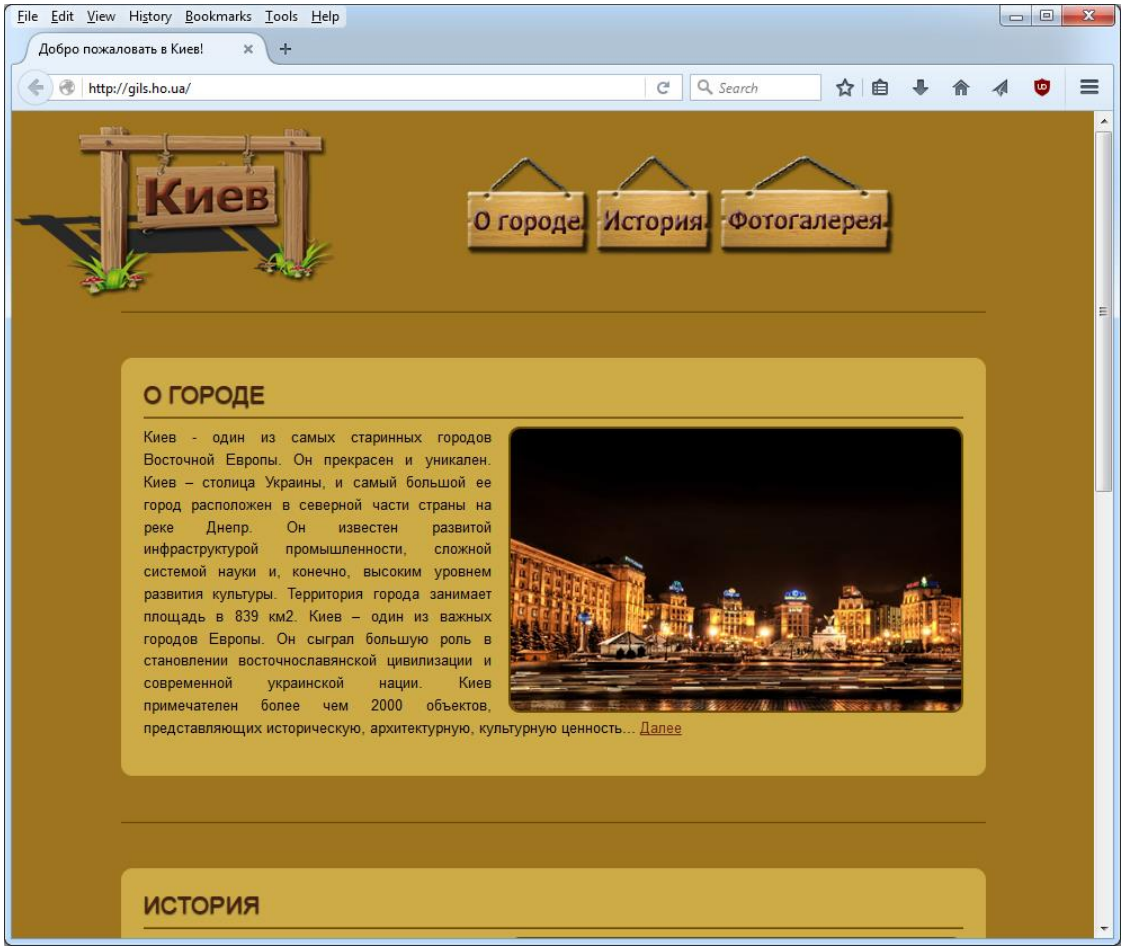


Рис. 31. Фальшивий веб-сайт, створений зловмисниками

У ході дослідження спеціалісти ESET отримали доступ до командного сервера операції Groundbait, який через неправильні налаштування дозволив створення списків папки загального доступу.

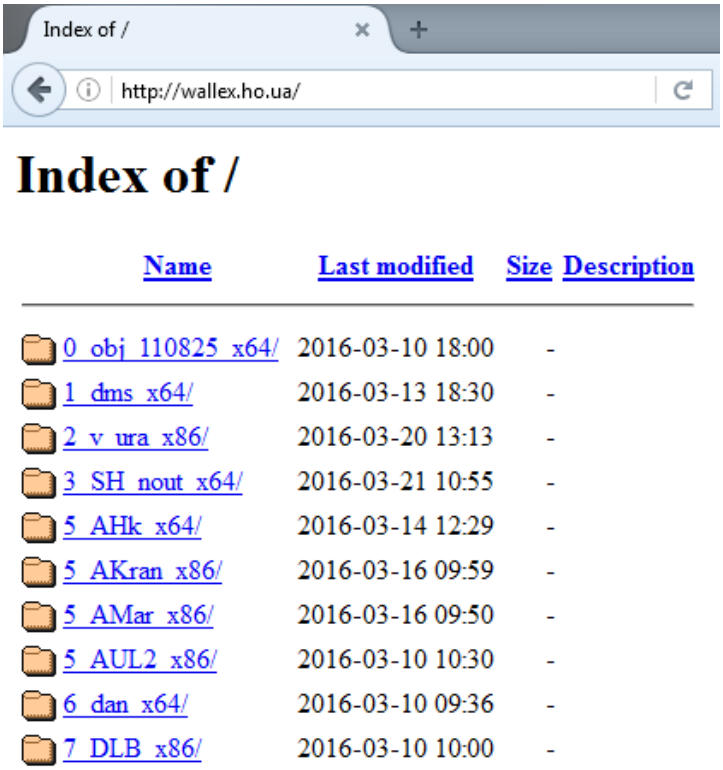


Рис. 32. Лістинг директорії командного сервера операції операції Groundbait

У певний момент коренева директорія містила 33 підкаталоги з окремою папкою для кожної жертви. Це означає, що сервер був використаний для управління 33 комп'ютерами, інфікованими загрозою Prikormka. Назва кожної підпапки містить ID оператора, ID кампанії, а також архітектуру інфікованого пристрою.

Кожна папка містить дві підпапки: `data` and `util`. У першій папці перебувають зашифровані дані після здійснення ексфільтрафії, а у другій — зашифровані модулі Prikormka.

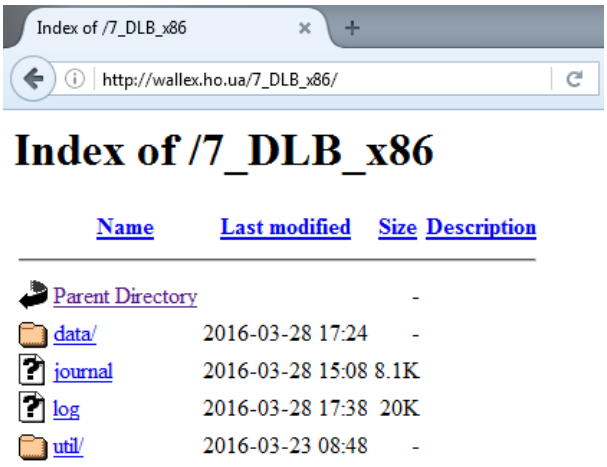


Рис. 33. Внутрішня структура директорії у підпапках

Крім папок `data` та `util`, підпапка кожної жертви містила два системних файли в текстовому вигляді: `journal` та `log`, розкриваючи цікаві дані про авторів шкідливого програмного забезпечення та їх жертв.

У файлі `log` також знаходився журнал зв'язку між сервером та інфікованим комп'ютером: зокрема, IP-адреса інфікованого комп'ютера, дата і час, тип запиту (GET або POST), розмір запиту, а також статус модулів Prikormka (у випадках здійснення запитів GET).

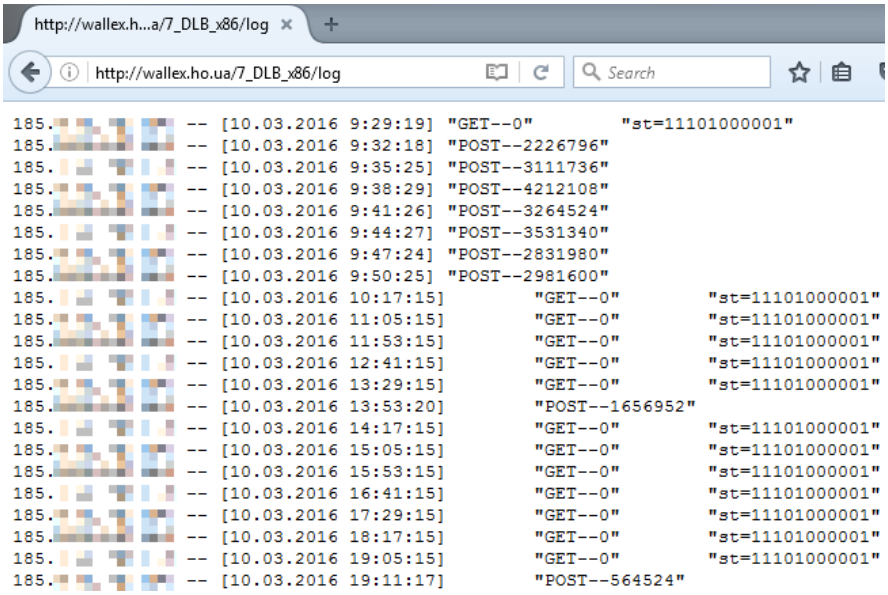


Рис. 34. Вміст одного файлу `log`, розташованого на командному сервері операції Groundbait

Файл `journal` містить журнал зв'язку між сервером і оператором шкідливих програм. Журнал зв'язку містить IP-адресу оператора, дату, час і тип запиту. Слід зазначити, що після завантаження оператором шкідливої програми, файл з ексфільтрацією даних отримує інформацію про видалення з сервера.

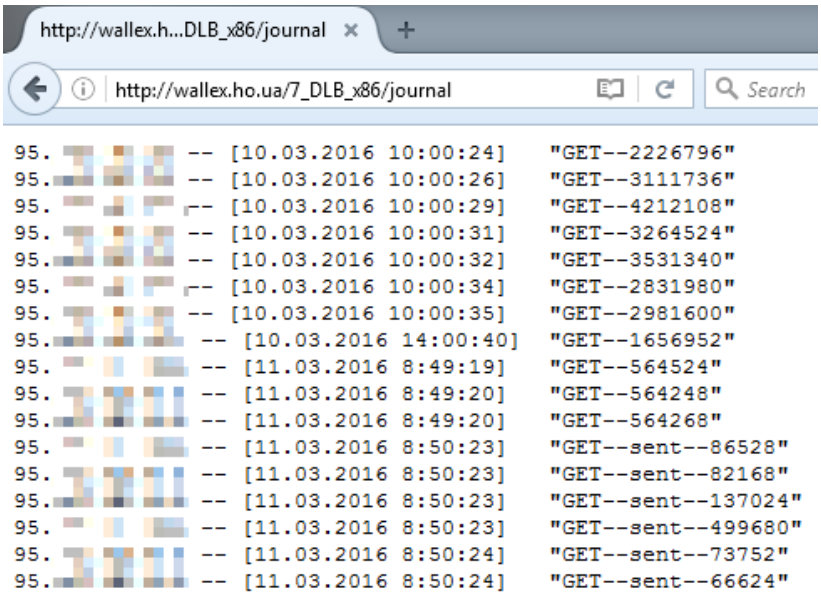


Рис. 35. Вміст файлу журналу `journal`, розташованого на командному сервері під час операції Groundbait

Після аналізу журналів зв'язків з одного сервера спеціалістами ESET було виявлено 33 жертви, які перебувають переважно в Східній Україні. Крім цього, кілька жертв проживали в Росії чи в столиці України — Києві.

Також аналіз журналів показав, що кілька операторів шкідливого програмного забезпечення були підключені до сервера з використанням різних Інтернет-провайдерів в Києві та Маріуполі. Деякі з них отримали доступ до командного сервера через мережу Tor.

Ідентифікація

У цьому розділі спеціалісти ESET спробують визначити походження загрози на основі ключів, які навмисно або ненавмисно залишили кіберзлочинці:

- Більшість командних серверів загрози Prikormka перебувають в Україні та розміщені українськими хостинговими компаніями.
- Зловмисники, які стоять за даним шкідливим програмним забезпеченням, вільно володіють російською та українською мовами, що підтверджують тексти документів-приманок та бінарних файлів Prikormka.
- Деякі з PDB-шляхів показали, що автори небезпечних програм використовували директорії з назвами російською мовою.
- Усі проаналізовані завантажувачі Prikormka містили мовні коди, які відповідають українській (шістнадцятковий код 0x0422) або російській (0x0419) мовам в їхніх PE ресурсах (Рис. 37).
- На основі компіляції часових відміток бінарних файлів Prikormka можна зробити припущення, що автори шкідливих програм працюють в східноєвропейському часовому поясі.
- Відповідно до журналів командного сервера ряд шкідливих операторів, які беруть участь в операції Groundbait, використовували різні Інтернет-провайдери в двох містах України: Києві та Маріуполі.

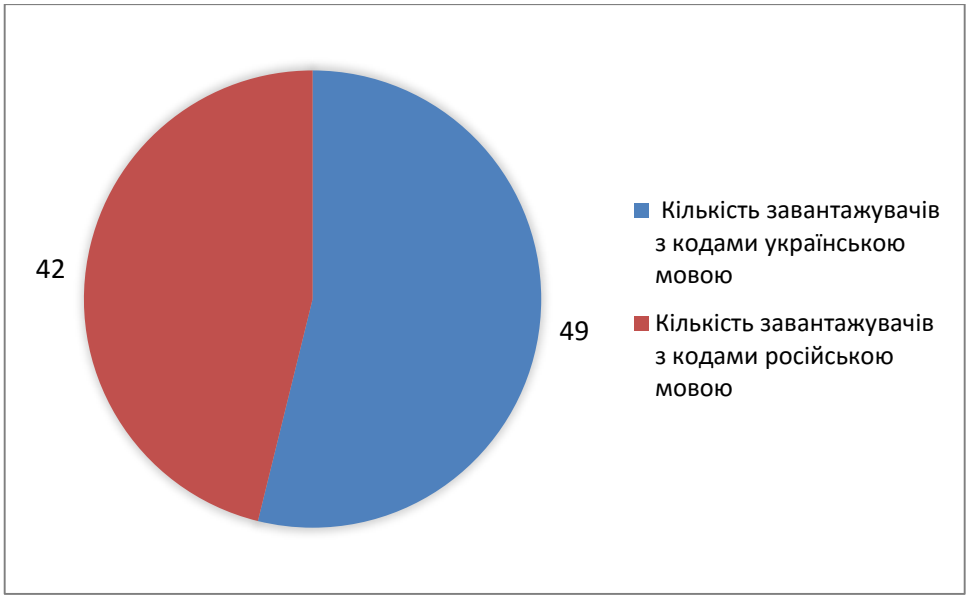


Рис. 36. Співвідношення мови кодів завантажувачів

Завантажувачі більш раннього періоду (2012-2015 роки) дійсно містять ресурси з кодами російського мовою. Однак з середини 2015 року автори шкідливого програмного забезпечення поступово переходять з російської на українську мову.

На Рис. 38 представлено розподіл годин компіляції зразків Prikormka.

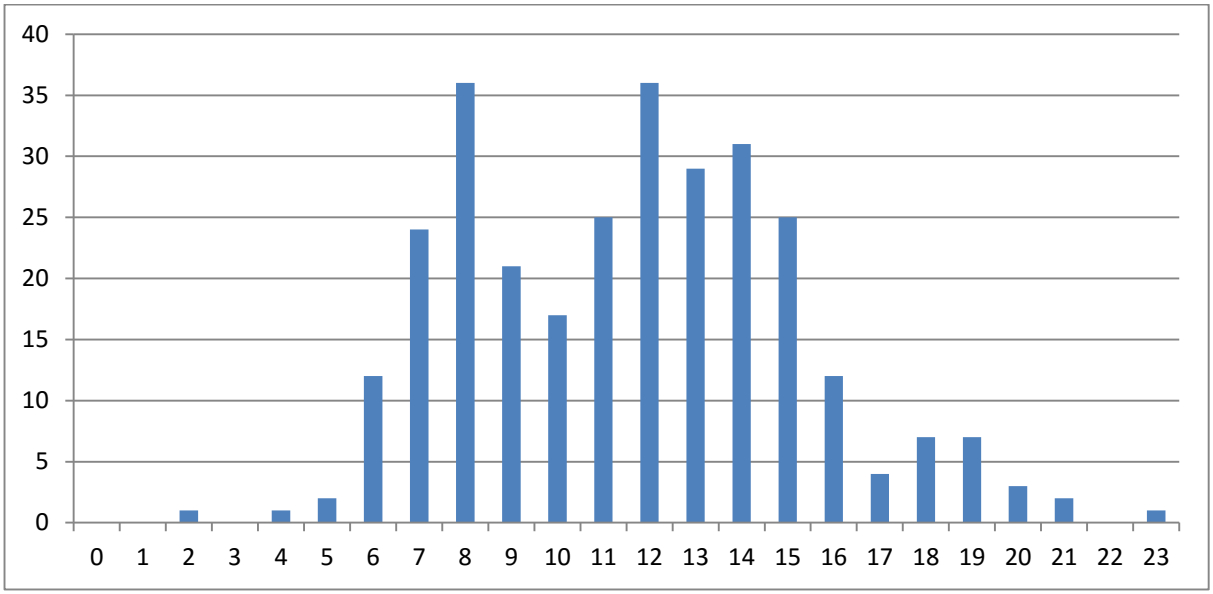


Рис. 37. Зразки посортовано по годинам (UTC)

Відповідно до отриманих даних, спеціалісти ESET виявили, що автори шкідливого програмного забезпечення працюють з 6.00 до 16.00 (UTC), іноді залишаючись до пізнього вечора. Режим відповідає періоду з 8.00 до 18.00 за Східноєвпропейським часом, тобто звичайному робочому часу в Україні.

На підставі досліджень та отриманих фактів, спеціалісти ESET прийшли до висновку, що реалізатори операції Groundbait зацікавлені в спостереженні чи шпигунстві за сепаратистами Донецької та Луганської областей, а також кількома конкретними цілями особливої важливості, включаючи українських політиків. Оператори шкідливої програми та/або автори володіють українською та російською мовами, та, ймовірно, працюють на території України.

Висновок

Дослідження атак кампаній та небезпечної програми Prikormka показало, що дана загроза є першим виявленим українським шкідливим програмним забезпечення, яке використовується для цілеспрямованих атак.

З точки зору технічного розвитку зловмисники не використали будь-які складні або нові методи. Однак це не має значення, поки кіберзлочниці досягають свої кінцевої мети: здійснюють крадіжку конфіденційної інформації з метою отримання власних вигод.

Найбільш значним досягнення авторів загрози Prikormka є непомітність даної програми протягом 7 років. Шкідливе програмне забезпечення з'явилося щонайменше у 2008 році. Цей висновок підтверджується відмітками часу бінарних файлів, даними ESET, а також використанням хостинг-провайдерів.

Операція Groundbait після операцій BlackEnergy та Operation Potao Express ще раз продемонструвала, що використання високоточних шкідливих програм для шпигунства під час збройного конфлікту є повсякденною реальністю.

Індикатори Компромісу (IOC), які можуть бути використані для виявлення інфекції, можна знайти в Додатку 2 або на github.

У разі виникнення запитань щодо теми, зі спеціалістами ESET можна зв'язатися за допомогою електронної пошти: support@eset.ua.

Подяка

Спеціальна подяка @TheEnergyStory

ДОДАТОК 1. ДЕТАЛІ КАМПАНІЙ PRIKORMKA

PE Часова відмітка (UTC)	ID кампанії	ID оператора загрози
Apr 19 09:11:27 2012	N/A (corrupted)	N/A
Jul 25 08:31:32 2012	SKt	N/A
Sep 13 08:21:54 2013	MNa	N/A
Mar 12 15:17:23 2014	Pgks	N/A
Jul 15 12:18:51 2014	Abk	N/A
Oct 03 08:57:13 2014	W_zp7a	N/A
Nov 05 07:56:00 2014	zma	N/A
Nov 05 19:30:35 2014	Psep	N/A
Nov 13 10:20:10 2014	hmod	N/A
Nov 25 15:12:31 2014	1ff	N/A
Dec 01 08:07:07 2014	hmyr3	N/A
Dec 05 13:11:35 2014	1ii	N/A
Jan 31 13:19:22 2015	1vo	N/A
Feb 10 18:31:49 2015	Pgad5	N/A
Feb 19 15:51:33 2015	Pkof	N/A
Mar 02 16:23:42 2015	Ptrop	N/A
Mar 11 08:43:12 2015	l01u001	N/A
Mar 23 12:46:24 2015	Asap	N/A
Mar 23 16:03:19 2015	P647	N/A
Apr 10 12:26:20 2015	Plg8_	N/A
May 06 06:08:52 2015	W_cu6a	N/A
May 24 08:46:38 2015	Pod13_	N/A
Jun 11 14:59:45 2015	Aste	N/A
Jun 21 15:36:24 2015	MVD_LNR_kontakt	7
Jun 26 13:25:22 2015	r03u0002	N/A
Jun 29 06:19:36 2015	Dmindoh_zb	7
Jul 01 12:42:04 2015	r03u0002	N/A
Jul 05 06:21:49 2015	Lminfin	7
Jul 09 14:48:56 2015	gm	1
Jul 16 14:29:29 2015	Lmgb	7
Jul 16 14:55:50 2015	Lrod	7
Jul 16 15:03:59 2015	Dmo	7
Jul 18 04:35:41 2015	Lsck3	7
Jul 18 05:07:50 2015	Dmo	7
Jul 19 07:41:54 2015	PMil_6	N/A
Jul 19 08:11:26 2015	PLmgb2	N/A
Jul 20 17:51:04 2015	Psek	7
Jul 21 06:08:53 2015	medium	3
Jul 26 19:17:52 2015	MDLV2	7
Jul 26 19:22:27 2015	OSCE	7
Aug 07 09:23:57 2015	BOY_D	12
Aug 14 06:11:43 2015	BUR	7
Aug 17 17:58:58 2015	RBx	7
Aug 17 18:32:51 2015	MRV1	N/A
Aug 22 11:35:37 2015	D_00732	7
Aug 28 13:42:34 2015	D_xxx	7
Sep 03 12:02:35 2015	zkonv	N/A
Sep 24 16:39:43 2015	L_mgb	7
Oct 13 10:52:47 2015	R_pol_x	7
Oct 13 11:54:58 2015	RF_lgm	7

Oct 14 06:55:23 2015	LKos_xx	7
Oct 21 12:56:05 2015	K83_mo	10
Oct 21 19:33:21 2015	DLB3	7
Oct 22 08:48:26 2015	DLB_sgrish	7
Oct 29 14:00:05 2015	FSfarm	11
Oct 30 07:40:28 2015	piter	8
Nov 11 08:57:44 2015	45K_perev	10
Nov 20 16:43:20 2015	30K_alfa	10
Nov 26 12:54:58 2015	REP_L	12
Nov 28 07:39:26 2015	L_K_geniy	7
Dec 03 07:21:31 2015	D_odSD	7
Dec 03 09:40:43 2015	L_min1	7
Dec 03 10:33:27 2015	D_newsG	7
Dec 15 11:48:39 2015	M_raz_	N/A
Dec 18 09:12:40 2015	7_L_xxx	7
Dec 18 12:12:10 2015	33K_pushkin	10
Dec 28 13:57:12 2015	38K_135_vnos	10
Dec 29 14:58:11 2015	Kvk_ham	7
Jan 12 11:44:22 2016	38K_83_parf	10
Jan 14 09:14:22 2016	L_ssa	7
Jan 19 15:30:41 2016	shubin	35
Jan 19 15:31:31 2016	shubin	35
Jan 19 15:33:35 2016	shubin	35
Jan 22 10:04:27 2016	34_Ffot	11
Jan 30 06:38:17 2016	MM_mmh	7
Jan 30 07:56:11 2016	L_m3	7
Feb 01 09:46:49 2016	38_Faro	11
Feb 05 08:00:05 2016	MM_1eco	7
Feb 05 08:20:01 2016	MM_1kur	7
Feb 05 08:51:46 2016	L_1m1	7
Feb 08 14:49:52 2016	L_ment	7
Feb 17 15:06:39 2016	sdd1	12
Feb 22 14:25:18 2016	L_rozysk	7
Feb 22 14:29:36 2016	L_rozyskR	7
Feb 25 10:26:58 2016	33K_037	10
Feb 25 14:18:30 2016	F_ego	11
Mar 22 15:25:59 2016	sgukiev	11
Apr 08 12:13:20 2016	avl	6
Apr 18 11:10:21 2016	L_ukrB	7
Apr 27 12:40:46 2016	puh	6
May 05 11:42:54 2016	L_gp	7

ДОДАТОК 2. ІНДИКАТОРИ КОМПРОМІСУ (IOC)

Користувачі антивірусного програмного забезпечення ESET повністю захищені від загрози Prikormka. Крім того, ESET надасть додаткову інформацію про дану небезпечну програму особам або організаціям, які інфіковані зараз або раніше.

Електронна пошта для контактів: threatintel@eset.com

Виявлення ESET

```
Win32/Agent.UIG trojan
Win32/Agent.XOR trojan
Win64/Agent.XOR trojan
Win32/Agent.XQX trojan
Win32/Agent.XRA trojan
Win32/Agent.XRB trojan
Win32/Agent.XRC trojan
Win64/Agent.DX trojan
Win32/TrojanDropper.Agent.RGH trojan
Win32/TrojanDropper.Agent.RHN trojan
Win32/Prikormka trojan
Win64/Prikormka trojan
MSIL/Prikormka trojan
```

На основі хосту

```
%PROGRAMFILES%\IntelRestore\
%USERPROFILE%\Resent\roaming\ocp8.1\
%USERPROFILE%\AppData\Local\MMC\
%USERPROFILE%\AppData\Local\PMG\
%USERPROFILE%\AppData\Local\SKC\
%USERPROFILE%\AppData\Local\CMS\
%USERPROFILE%\AppData\Local\VRT\
%USERPROFILE%\AppData\Local\ioctl\
%WINDIR%\ntshrui.dll
%WINDIR%\hauthuid.dll
%WINDIR%\hlpuctf.dll
%WINDIR%\atiml.dll
%WINDIR%\iomus.dll
%WINDIR%\swma.dll
%WINDIR%\helpldr.dll
%WINDIR%\rbcon.ini
%USERPROFILE%\AppData\Local\CMS\krman.ini
%USERPROFILE%\AppData\Local\VRT\_wputproc.dll
```

М’ютекси

```
ZxWinDeffContexLNKINFO64
Zw_&one@ldrContext43
Paramore756Contex43
ZxWinDeffContexSMD64
ZxWinDeffContexWriteUSBIO64x
ZxWinDeffContexRNDRV45scr
ZxWinDeffContexRNDRV45snd
ZxWinDeffContexSkSwmA
ZxWinDeffContexKINP64
ZxWinDeffContexRNDRV65
ZxWinDeffContexRNDRV65new
ZxWinDeffContexRNDRV65xyz
ZxWinDeffContexRNDRV65xy
ZxWinDeffContexRNDRV64
Client67workProc98List3To
```

Командні сервери (C&C)

disk-fulldatabase.rhcloud.com (IP: 54.175.208.187, 23.22.38.222)
wallejob.in.ua (IP: 185.68.16.35)
wallex.ho.ua (IP: 91.228.146.13)
gils.ho.ua (IP: 91.228.146.12)
literat.ho.ua (IP: 91.228.146.13)
lefting.org (IP: 91.228.146.11)
celebrat.net (IP: 91.228.146.11)
bolepaund.com (IP: 91.228.146.12)

Сервери, які використовувалися для відправки фішингових листів

server-eacloud.rhcloud.com (IP: 54.152.171.48, 54.163.210.39)
easerver-fulldatabase.rhcloud.com (IP: 52.23.164.7, 23.22.221.237)

SHA-1 хеші

Завантажувачі Prikormka:
42041871308B5711041B7AF69B78F45DF642546C
37F75844C0D0F7F80A699153AF131984D2CE2B6D
029F054A52FE93B0CD6C4D1D815A795EAE9CAAB4
66C143D7C33666903B174F4B94D609BE8791914D
60351035ECDEED071E3FB80AFFE08872A0B582C9
0296191B323900B2BC014E2ACB5E0614C679B682
1BF0E90027EF798727A4496B1928F1FA79146051
76CAE58E4DF4D029155BF2E44BA0F8075DC99020
C0FBE31F1E6E56E93932076BA55A5229E22B5C4A
CF09B0CD03C9D0553F0B82827C989D04F1A1FAF1
7C28B907E1053F825478A74FDC1090FBF71DD878
D7F35B66C554EE1076279DF54C4E931651A7A211
2B0FB236DDC0098ADDF051531912FC2601FFCCDC
EAB122E5857DF838469B5B00DA0A3BD06DF8DA05
00BCCEBB7614BA270CA2908EE5711F25D3740E7E
F908824DB35EFD589449D04E41F8BCEA057F6E52
A8CED2FF8F3D4B77160CB81843652D971469A30B
6002357FB96A786401BAA40A89A85DBA3A7D7AD4
E3E9CA2AC83CFADD80FECD002B377B6B41AC5250
EAFC458AAC3F1564E940BAC7D45C1E659636CC86
FCBC8C75246511F9E4D49FE501F956A857FACE84
803C48A93785581AA89422B6B1E73677BF8DC749
87C34623EBEC481FD430F6CE26849220C641742C
A1EE4E4BA27B4035F29FA6AB943AE072D42E65B8
19AAB5FAE0809F87EF27A18208A3C0C52DEA182A
C88218C2C23555D5E39596B2110BDA54A7AD50DB
EC16141D6C0399B74A26B7B572580B3AC4CBC811
76B77E40182DA242307272B9F77132ABB0B46515
7AB44936E5545C5778C697ABCC20FD8955E35F36
86DD049877B564158020AB9B1A6CA3C30371979D
8665C7A753BA5F619FE79D52DC49724F17D81DAC
8839ED42EC1440CBF30CC345F11B88450EA8FE46
4D2C8CD6C514202CBC133347E2C35F63F03A77BF
CDF0734730EA786AD2D3B0E9D0D82F85D3C4AD07
99345C5E6FC6901B630C044DD5C6A5015A94B046
93FE501BCDF62060798E35643B7E5F4E3FFF05A6
1287205FE5B83583CB28D39D965D182EA1DFCFDB
C0C4DB689F393A26611B7F8FE08F38B456A173DA
3F867CF4AE4B1232B08E40ADABE7BC21EF856FE2
E9A2B1611EDC105FBA65AFFCDAB062D6FA5C67B0
ADDF8193442D145C6BCB4C54B95A5CFE759C6436
CD5AA66AD7C8D418F19B486211591E31B5B74AB6
8A01C06DF6E59F1513146DFE07936E4ACA59B152
E35081B99C5445952AD4E204A4C42F06D7C3707D
A6D8431EFBA501864C4646A63071D28B30EEBF99

613F631D0E384954D2FEA5BE39124AD821C8E5D6
D45CECD9DDD79259C6518300ED77257A9ABBDF92
642033A50EF2C51E1F391D85ED870B09A308469A
FD95C6B33AF4B29EFBD26D388C50164C3167CB68
9A578C7C305BE62167EF87AB52E59A12F336186A
FE9F5018198567F3D3FB3AA09279C65DBE981171
62487DD8EC172462F9B4CBB790EF6F7878D20352
E397F1D784B4A9EEE7EEAC427C549A301DEC0C7C
E8A2734C3FFECB76DD4D1C28D646EE59188BE7BF
8DF79B2734BCD83B3D55FF99521D10E550DFCFF3
64D31BBCF8E224E06BB5F1B350D2F18BFDD78A8E
D5B785F8F92C7588CFAD7A1A21DAFFA6EB9CFA5C
8327A743756FA1B051725BF8EC3FDD9B9E844E9A
98440EC18A7E78925CB760F5016111115C89F1F8
6E56BC6023085D6E88668D1C66B91AB5AA92F294
160CF2ABB25495188A0ACB523BD201B0369CFFD2
6E5A098A3EDDEEC2E4986DE84FB00D7EA7EE26B8
8358EA16A0DE64994FBECE1AAC69E847F91BB1B3
3A6C8CB6688E2A56057BA9B3680E5911D96B2C8C
AB011CD03B3F211F43930AABD909B5611A829D9D
279711B6828B6CF642C0DAB4D16411C87956F566
2BF9CA8B16BCD679AFB6E9E53C3BB0B04E65044A
9551C390B2DF178DED895D531F440FDDBAE122AA
BB8D93A4049968C6D5A243DCFB65A6F4B4DE22A2
80CB14652E8251C79187DF8A01D29ABD46A3118C
6E24C2403DAFAE05C351C5A0A16E2B6403E0F398
09EA7B2F67797915BBFED16F0B21E4E31F4980A3
0AA48DEE8F528B037D8D72AAD039BB2759F362E3
40D7D09053BF60925CBB820417A42DBC6293E017
A6600BD9752E041ED7EE026123A60B19C96259AB
506CCEBDAC5754D1E20D9C3FB280CEC7782EEA6E
40F33CD2AD98FE1E6BF4AB199021498F9E3125A1
9F03A4E0ACD38635104292B8054485E6BF898C48
B373BF4B3AA28FF6D373DA5EAA848AF9772F6454
FD83C2484E2986F22B09623E5971AA54FBD8BCD3
065B075293968732F2BE433B7B492869E4260EE5
B358687593FEBDFD0E1858726098DCFD61D9F8B5
FD2FBB8E4676673A35276B46F2C74562703BCF39
CCD19FD4A1408FCD855B7909578340846904E707
9D84665C00F81C2835E2A41711A139547351D850
69536CAF0522C1A915D6AC4C65177A26EFA7944B
243421FE7C1FC007EFA0C9CCAB6F6E2A0C94FCC2
5B7D6D7C3C4AD74A7F1E32B780776DB41FF18DDD
4418A32BBD215F5DE7B0063B91731B71804E7225
EE1E5D95FCAD429126944804D80D7C2412AF492E
E494328255EF2B9ED9B332EE845513A93339217F
6B53A3A3CB9D87D5925C82839015DAD16042C2FF

Попередні версії Prikormka:
1B8BC6924F4CFC641032578622BA8C7B4A92F65E
B5F1B3BD6AD281C8EB9D633A37E0BE63B97A8BEB
BCEDAB81CC5F4D2EA1DA8A71F91DF6E16362723B
DC52EE62B94DC38790C3EF855CE5773E48D6CD55
44B6B8375CF788076C0DD64A93E27F69A01F5DFD
539033DE14539D485481549EF84C9E49D743FC4C

Модулі PERSISTENCE Prikormka:
AD9A6F7BA895769844663B4936E776239D3A3D17
E1B5CD1978F6C6D72AA6B07ADD1EE83E9BB8480D
6E312A999EE7DCD9EC8EB4F0A216F50F50EB09F6
8F8BD3C4CE2F932ABFB31B9F586C40D1E22EE210
3F8D8B20B8FCC200939BBB92FB3B93BB3B4ECD24

756730D1C542B57792F68F0C3BC9BCDE149CF7C6
4F1441F16E80272F488BB114DB6508F0BB9B9E1B
2E1C7FFAB7B1047E3438E6BA920D0914F8CC4E35
3C9990B5D66F3AE9AD9A39A10AC6D291DD86A8F9
CC7091228C1B5A0DAF39ECDA570F75F122BE8A16
26FAEAAE2C042C0A416287A7C54D63D5B4C781B3
854F7CB3A436721F445E0D13FB3BEFF11BF4153D
0596EFE47D6C143BE21294EB4E631A4892A0651A
7DAE2A15E364EE06C9301236AE8FC140884CEA95
C2F720DEF2264F08E5211671D46E73311DC6C473
36215D9A691D826E6CEBC65925BFA6B579675158
0354A768508F6B9D88588641397B76A0CBB10BF2
1790B3D73A5DD676D17B39C01A079DEBD6D9F5C5
2F1E4AF1A5A95B3483E901ABDD96454C57419BA4
53174F09C4EDB68ED7D9028B86154B9C7F321A30
FCD81737FF261A84B9899CB713933AA795279364

Модулі DOWNLOADER Prikormka:
D12CD6C4CA3388B68FCF3E46E206064CAA75F893
C2EA09D162BDAD2541C97D30A4E171F267305671
C10D6E4ADB3B29C968D7F3086C8E7005DD1E36F4
CE4605994E514086ADA5A767296DB66D7EA84175
148218ECDDE9ECC19B1343080884EB819783D9B2
5B256971F332498ACC833B36CBE9AD0CEC71384C
4A8452575FF69BDD0806AA8915E459E8ADC66DF1
04DFC621649511E1AB6CB800124DD5E2874A1629
D51863CBC1AC4BFC2B87F247DC75975E2A9CD992
C8AF6A8270CBD030F09C24888480AEF093ACCF48
EF127184967BE14A3719978E0236FFF5C0AF811B
2FF9E3AB4912A4AEA3C511D9355B8EDD13888E2A
40B163E8E74397E69F18805BD7DAB67F06D3D9E2
A8DFCD6CDB0755966F3D6766B94989CDAA0C35F9
6D4A80FE57D57B43DAF85401DFDD2CDA48D1F023
7844678942383F8116BAC656BC56D4B230FF62E8
8B9460431296DAF13BBE8D0F81EBFC19A84BB741
995EE9772DDDF2D6B4A55ACF26FA41F40786532D
ED7B147766C1370367D277F7BA7E354DBDDE5E09
37316B972F5C22D069764800475EED7CD3279802
1DF0B7239E48CF8E7391085BE5B835C892A5B3E8
0323D1C5D565627C32FF08780A59EB45D6C0C7C3
4673475BD3307FE8869ACA0402B861DDE5EC43AC
F38CFC487481D2B0167E5B76F06500BC312081B6
35159C96F695B96773C5C1DCF8206DBE75A83D86

Модулі CORE Prikormka:
2A64606DB1DB872E7176F0C6C3FF932E2146BFC9
328DE44A4B6140EF49CE1465482EFE0E4C195399
520AA689066D0C69F6FD9C623E263211022CCF21
790367A2032951488FC6F56DCF12062AE56CAA61
551CD9D950A9C610E12451550BD6A3FBF5B00B77
EF3244AB1DF7D74F1FC1D8C3AF26A3D3EA4364A5
1636112D8441A6616B68CBE9DC32DDB5D836BBA1
8A57E5EED18A6DB6F221B1B9E8831FE4A9CAD08C
DCB813E5D2A1C63027AADC7197FD91505FD13380
A360EAC305946FF468E1A33E84ED38176D95CAC9
8F67C4BD2EE7C68249DCD49AD7A3924D3EC6810C
C020EFFD3C7AD06907ECFEA424BE1DCB60C7447D
D2A98115DF0C17648CCB653AF649D24B528B471D
D7EEB8DB22AAD913B38E695A470E8B2F1440D4D3
154AA820D552ABD65C028DED7E970C8DEFA8C237
83B492A2905CE6ACFADE43AB52BF52E6F02FDCD5
4F945A3B3EB058668C3DFC0A8469B42E16C277A7

963963004E4CA0D966D84324EC8ED3694F6A7F5B
9DE8860AD499E64F8BDCFC800DDAFF49D4F948E5
C9C2510654081D621A5B1768520D7D7C04219FCB
9D025A015FDB720C0FDEBCFE54661F3ACED94E3E
D09B6194453BFC59EB438E455D14621B280DF4A6
1A865E934EFF339A826979C70A2FC055E3C9D12F
4C5F412C915FB3F178A81BC4FBDA336F69A22086
7372639A9E5C274DFFAA35ABF4C8E7A0BEBD4305
311672ECB756E52AD396227DD884D1C47234961A
7A22E549BE02F7F4753BB9CBA34079CEB15CA381
6AB00FCABC6BC06586F749F54C4955592285608C
66248AE0A3D6B5091C629343CC535F98E08A2947
0DD8E1922CEB96061C9F6678728DD45CBDC6F675
A093993B9488A9427300B2AC41460BE8164A0F9A
6D861826206D834A224583898BE6AF1A3D46E7CF
64679BDB8A65D278CDA0975F279D8881E1ABD40A
92476C6AE5F976C58D11BDD956878451F361776D
202637EF3C9B236D62BE627C6E1A8C779EB2976B
C41BB97C203D6221FB494D732CB905FF37376622
986E739948E3B5C303F7766F9F9AF3D2E1A5BCA7
3AB61FEC417686AFC1AC430AAF5A17254D05A14A
0D7785E53AB1A7F43902AFF50E7A722C0E0B428F
B5EEAE045F1082438E4C7B7F12F7F4630043A48E
57E345893F508F390F2947E83092A47D845EA445
C9756E95679EAD052D53ADCFA39BB4B1402C9126
D864067BFA52383BC012BA1AAF8FFB893D419C07
CDD58347F873EB7E0BC602DA9930A519683C67C7
DFABE31E58334C873AEDD361D69D5C80016F9F42
625D822EE0D95C6E581B929C6C4E4B44D749D2BB
A224A76DABE62BD7CA055CA1119108AD5812AF06
E4C56D11E84497EEC3E275043E36845EB2F3F57E
B43713CBD307BC12AD7BA61C87975F74221A3439
AED9C3BCA2B42889A9110B92D3D31B5FD3324BDF
6AE2C768D932EDA538983DD7A50CF7DE14BF54D2
BE73A2C17AAE689BC1A20761850374636B67BF0F
80FFA899CB3A6595FAFA66421BCCD6E5AAAD8552
7C5F7296DDDA9B188B572DF348843F822BD6ED21
F9EB705D8A1EDC7FF9B93D9CF9211840C4482865
7979BEC789770860A6F12B7A7D41470DE4AFC873
6DF75137E8966537BB921EAB30DF4F7BC2C6FEB4
2115C50CAF8D1B365D78818DF84A8CE29F7FD9E8
AFDAD724A2C351C750DB43688D107B1300B1D1D4
64002D2C4C6678776C64BB018736C9B0745F47F4
7843CB7DE03C8B564FD72D923B4BD6D28A466A3C
EB4647CA60FEA9049A34EC59D9658946A2C26D9D
ED3D4EEF28174F60F1653F35000B871F6E023D21
860D0CDFC065E91083979DD50A72251C26A638A4
FC2C689C507FED54432AD1726E524B38F52B187A
D219640BA205A7013A23BA19CD6C2B32439F105E
DE60C2A81AE2F3E5DBD2B2D0DBEBDB56FED62F7C
D38FDAE48EABF2642F3327FAC865B079233CC7C6
B23995462751EDFAD19B72BEA4A047CC89533A59
88ED6686CF59F12AA984216EC60097C4BD319007
DEF9B207BFD7C6D4B216DF2B37C33CD851DC7FE1
8D49305FD140B179D2293FBAFF6E7CE46A03AF16
F35B1D2165EC00A56EE6DE89D09963DD3FD02744
B42234F5A5EFB6423E9D4904BA282127F1282C8E
326ADEA3AC1F8FAC3B522E6B47941263DA110A42
3E023A83EAA85A77B935B2D3A00AEB5B1ADCD9CC
129B852E62CB7BF487D5F37E17F6E3CC9A838DB8
F030559F81B8DC3CC0DED6C46C6D1BBB67A2CA65
3C904AFB938EFCF210F388E5AA46379AEADBCD50

D8921385ADAFF131C9D452A4D9BBA2C7D755880E
915F7F5471A94A6E095EE8D90FCFE84E7A5FE1D5
0DB71AA8B51FAACEA7D4C5819EC6AF9C342D02FD
A4847B06E603E90640051FCDD5D1515F007F7BD5
7C9E4CC3F5B260439D69E93376AA668BF32123D0
3246B5F43756DC8DC4438933005DF66A3C8CE25F
E97B383E3CF55D0792F22D57273C18848B849C6E
7C6FA82657B291FAFE423B7B45D0ED732F4D5352
4595EAB593594860985F5FB501B85386F1F1A5B8
45F1F06C3A27CE8329E2BDCDEEA3C530711B5B72
476DCA86DE7AF1F15327084021A3BB7F42818248
70A362985D5237ACD6282E16A238B0FDB1002A1F
73596D1587549DC234588FCB5666BEEFD7C90D81
97958B3124EC5DCAB64DD88A1E97E6B585B04628
B47640C4952ACC2705F7EAD9E8EAA163059FD659
596F945AB52AE0E780905E150ACD2017AB2ECDFC
5CEFFF9C7D016364D40F841CB74D65BB478BA0C6
424DD485FA8572DB84CF6845C27C1F8679A61AEC
099C5611F3BDBB8D453DFBF7967F30891906FF2C
7C2587B85178AD89389D957F11AF1065C46F66DB
840AFB728FDA57195E53F225CB3F6E788B96A579
12ACC64605D4FE2F3CEEEFBD0A7C4FD655E6AEAA

Модулі DOCS_STEALER Prikormka:
BA434FB6169E8A1785E353EEBF9B907505759A07
A34BD2A059F57FB1FE281A2BD7247A9A72A467B8
04DEB60B6A1D53448EFFB34EA7C55E6916FE32B1
C75D8850273431A41F0EFCF8F74E86BCFE1DFA5A
7C9CB1619FFCF36B32273E1A78A58D817D2B7C8C
A580856FA6AC3159F0A7E91D5992810B953A36A1
5C82CA8B2E8320E6B6C071CCB0D4EF9B03001CAA
7275A6ED8EE314600A9B93038876F853B957B316
9286B96452C519D5E1E74D1CDDBDD76B51F4FBAA
FAB3B3371AA5878B6508DA487735E3A674A9F61B
0D4839F99C30AD76E082851A214A32116CE932A7
652B012E0ACACB78221CAA7A3C3EE461F07264EA

Модулі KEYLOGGER Prikormka:
BFDCD0A3F7495C43D8D42B4272BDC90695DC44D7
CC42C6BEEB70D3A9BC7E1159C644E54DE2BE5CBC
6A4F24665569DD61FD29AF8FDCB3E2C90961DFF0
D1DA3076830813EC6FFF0B0DE3462BB5B713A090
E6D92C025CF726B08288B6798AEEFCF550D51C31
0B81BA761C6BA88C0AFC682693D99355E55F5A76
0CDC66ACBB5B7D6FAA85F7DF8D747A96CED7A9BD
194316ADC74AEDED98EE2696B4AB54900A6EDF15
45959818DBA4924E129E22CF1B0BDF02C2DD7B49
820EAC424FC27296FE725E1C5DAA8F6C53E104A7
25D6F1EFD758AACE399C6D62A89BE039281CFF69
722E1CDA3C516D43F17A6D4F5F1390D16113BC30
DE966273DD5AD4DAA01562109932EBD39A13A5A2

Модулі SCREENSHOTS Prikormka:
645DFA35E41F6442793CF7647A75956E05563DE8
AD74ABEA34A20D0196A152E6668E3C29135B22D4

Модулі MICROPHONE Prikormka:
FCE83DF7018A49072F9A28A8E135EB00C011D9EB
2C76974722287C7CDB0FCA2BC6CCEDEE62E77D24

Модулі SKYPE Prikormka:
C3AA3DBD33751F85002F2F65562098F516737435

2A0EA9E0F3F8E6507D212640594ACF52910275E9
1BB3BBCA79BA45E4215DFC2A6960E03BA60A2B71
0CB528C69706A6513A0E70D3A07A75822F79E6EC
423BCEFC82A14258BDC2CD9740454D28F894DC06
FEAB6E92B905114980B5633F8742E4A7DCD0B4FA
BB6CE0957F7E8430007FA4DE1E47C190E1C97AC5
658DF9B4BB13459A9507466BB7D22B723C85D1C5
6C24E244A0DDA2CADED4D1B5CC8B820A46DC19F4

Модулі LOGS_ENCRYPTER Prikormka:
D5C2C7C3D670D63AD6998848747A0418665EA2CB
352C36ED1BF7EB74C9649615F9A40C13D80EE55D
6740A385AB33B9CC3EC22FB7971F93538BE44997
22F10F17AB9F18D9BF1FE9EEEA413A9787B29D4C
E95458CA9663E4FAB94DD232121D5E994A76015D
2BD3FE012486BD89C87858CC4C3DC9D86742738C

Модулі GEOLOCATION Prikormka:
50CCCD576A815AC8EFFB160A628646C876DF8CB0

Модулі OS_INFO Prikormka:
4B8EE967F44ECA2EEB3B8420A858CECFE0231208
72C17994336FE4E1B3CF0D7A6CBC45AA43A8DDF0
824F0E198A8A6E08FB95920AEF06870A6305FE3F
6C902496AC1FEF60D343B03822F49DB5F66BE038

Модулі PASSWORDS Prikormka:
B986114C5173052FCB9583A55D5099D99B709352
17F5E1FC52D6C617CD81B0983B70FAC7A60F528C

Модулі FILE_TREE Prikormka:
3EDD14E6FA0297ED3162D7F119D8D126662ED28B
2A5AF8E43887051C1F1B488756AAC204B95561CE
4E40286676FCBAC48070BA86B72761A21AC2466C
3E4BE58421DBAEA7651DA13B16CB900DB82A7DEF
D1396938E981DD807103B7B9F9442B99952C21AA
74CDA4D4C776CA2A661AC49B6D0E0F0560380A04
8EFDC716FDFD704EC0296860E61AFF9C952946D4
93E196B59771647828BBC3C3B61831150FE1FE02
8384ED4EA9E299306F15A1082231C427A8742271
6E70BE32954E41FAFFC496EAF890B279832B4530
8EA98A8D3D8F62C4543B3DD36E6D6F79F1ACB9E7