安全加社区

公益翻译项目

2016

Operation Groundbait：监视工具分析

V1.0 版本

ANTON CHEREPANOV,

2016 年 5 月 17 日

文档信息			
原文名称	Operation Groundbait: Analysis of a surveillance toolkit		
原文作者	ANTON CHEREPANOV, ESET	原文发布日期	2016 年 5 月 17 日
原文出处	http://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf		
译者	安全加社区公益翻译组	校对者	安全加社区公益翻译组

免责声明

• 本文原文来自于互联网的公共方式，由“安全加”社区出于学习交流的目的进行翻译，而无任何商业利益的考虑和利用，“安全加”社区已经尽可能地对作者和来源进行了通告，但不保证能够穷尽，如您主张相关权利，请及时与“安全加”社区联系。

•“安全加”社区不对翻译版本的准确性、可靠性作任何保证，也不为由翻译不准确所导致的直接或间接损失承担责任。在使用翻译版本中所包含的技术信息时，用户同意“安全加”社区对可能出现的翻译不完整、或不准确导致的全部或部分损失不承担任何责任。用户亦保证不用做商业用途，也不以任何方式修改本译文，基于上述问题产生侵权行为的，法律责任由用户自负。

摘要

Operation Groundbait（俄语：П р и к о р м к а，Prikormka）是一个针对乌克兰特定人群的持续性网络监视行动。此行动背后的团体已经开展了有针对性的可能出于政治动机的攻击行动来暗中监视特定人群行为。

本文基于 ESET 对恶意软件家族的研究，介绍了 Operation Groundbait 的相关情况。其中包含 Prikormka 恶意软件家族的技术细节分析、传播机制以及部分有价值的攻击活动。

主要调查结果：

•从 2008 年开始此类恶意软件大多数出现于乌克兰。

•Operation Groundbait 的主要目标是乌克兰东部地区城市顿涅茨克和卢甘斯克（这两个市经过公投成为独立的人民共和国）的反政府分裂分子。

•其他目标，包括乌克兰政府官员、政治家、记者等。

•攻击很可能在乌克兰境内进行。

安全加社区
公益翻译项目
2016

1 发现

2015 年第三季度，ESET 发现了未知的模块化恶意软件家族——Prikormka。通过进一步的研究发现，这种恶意软件至少在 2008 年就已经开始活动，且大多数出现在乌克兰地区。由于此恶意软件在 2015 年之前感染率较低，因此在很长时间里都未被发现。2015 年，此恶意软件的感染数目激增。

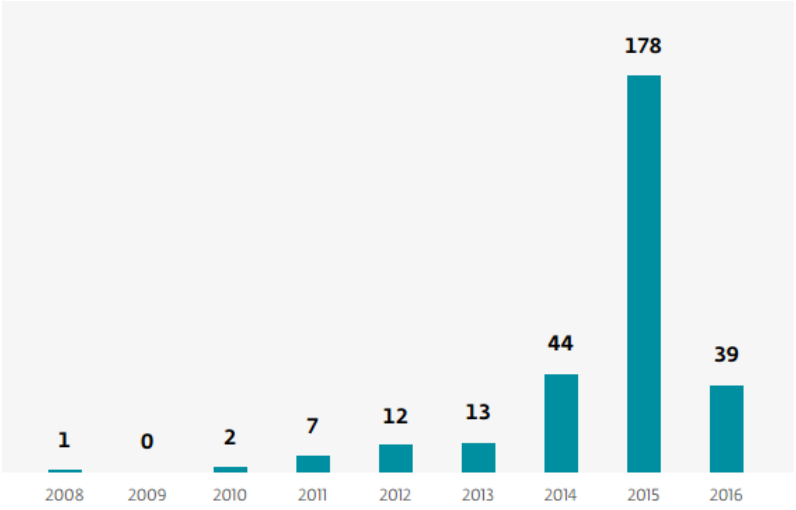


图 1. ESET 检索的独特样本数，（以年为单位，基于时间戳）

图 1 显示了 2008 年以来每年编译的 Prikormka 的样本数（根据 PE 头文件时间戳标识）。但是，在通常情况下，其自身的时间戳并不是一个可靠的指标，因此本文的数据精确度由 ESET LiveGrid®遥测证实。

在实验室分析了该恶意软件的样本 prikormka.exe。俄罗斯和乌克兰语言中的 prikormka（П р и к о р м к а）含义为暗中监视，其本身含义是一种扔进水中来吸引鱼的鱼饵。在研究过程中，我们使用这个代称并将之保留，因此恶意软件的名称分别的 Win32/Prikormka 和 Win64/ Prikormka。

APT 攻击的普遍特征是低检测率和多年隐藏的特性。针对此款恶意软件的调查活动和 Prikormka 的活动行为表明此款恶意软件可以在 APT 中使用。APT 攻击通常包含多种目的：监视，信息窃取，破坏和间谍活动。经过对这种恶意软件家族的战术，技术和程序进行分析，结果表明此款恶意软件的目标为个人而非公司（即使在企业环境中检测到 Prikormka，也认为其攻击目标为个人）。分析过程中未发现任何横移技术（网络攻击中的一种先进技术），因此我们怀疑，这组恶意软件的使用者在乌克兰，其中大多数受害者也位于乌克兰。出于这个原因以及它的攻击性质，我们将其分类为网络监控。

2 活动

安全加社区
公益翻译项目
2016

在这部分，我们将展示最值得关注的和突出的活动及与这些活动相关的诱骗文档。下图是基于 ESETLiveGrid®统计的国家检测统计：

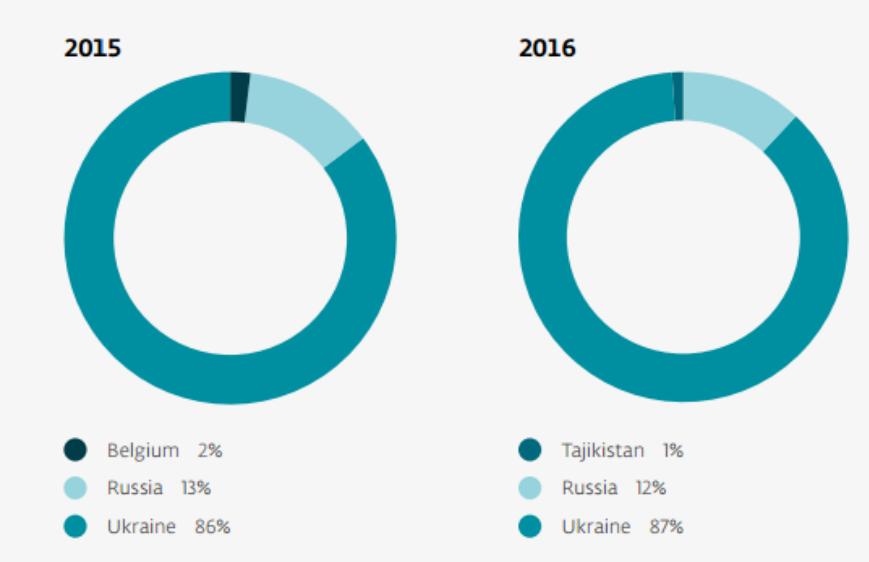


图 2 根据 ESETLiveGrid®的 Prikormka 恶意软件检测统计

根据遥测，大部分 Prikormka 软件出现在乌克兰境内。此外，研究表明，此恶意软件背后的攻击者使用乌克兰语和俄语，并且对乌克兰目前的政治局势非常了解。

想要知道在上述国家受攻击的类型，这里将会对样本文件进行分析。

Prikormka 软件的主要感染媒介为包含恶意可执行文件附件的钓鱼电子邮件或者是一个指向远程服务器的下载链接。当用户点击附件后，会看到一个打开的文档，Prikormka 恶意软件将自身隐藏在这个打开的文件中后台运行，打开的文档主要诱骗受害者、分散他们的注意力。是否能够成功感染取决于钓鱼式攻击的电子邮件的质量，当钓鱼邮件和诱骗文档与受害者相关时，攻击者更有可能感染计算机。换句话说，受害者收到一个和自身有关的邮件附件时警惕性会下降 。因此，分析这些诱饵文档可以推测出网络攻击目标的信息。

在每个 Prikormka 恶意软件样本中都包含一个特有的字符串，即我们所说的活动 ID。这些活动 ID 是唯一的文本字符串，用于标识 Prikormka 的感染目标。通过对所使用的字母和数字组合有时能够推测出攻击目标的信息。

目前为止，我们已经确定了 80 多个不同的活动 ID 及这些活动 ID 相关联的诱骗文件。据观察，通常是一个活动 ID 针对一个目标，其目标可以是个人，某些实体或组织成员。这意味着一个特定的活动 ID 可能会出现在多个计算机中。

附录 A 中提供了更全面的代表活动列表，同时标明了活动时间戳和唯一的活动标识。

在某些情况下很难确定目标受害者，特别是在 Prikormka 已经被安装和激活的情况下，然而，在网络中存活的 Prikormka 目标中，我们已经发现了包括乌克兰政府在内的高价值目标，其他值得关注的目标将在 Groundbait 系列中提及。

2.1 反对分裂主义活动

Prikormka 的主要目标是在乌克兰东部的分裂分子。2014 年以来，这一地区已涉及武装军事冲突。2014 年 4 月，乌克兰东部两州宣布独立：顿涅茨克和卢甘斯克。对此，乌克兰政府将这两个实体划分为恐怖组织，因此，这些地区被称为反恐行动（ATO）区。2014 年 5 月 11 日，这些自称为共和国的当局举行了一次投票以寻求合法化建立共和国。

Prikormka 攻击中一个比较明显的特点是使用的大量诱饵文件，这些文件使用了顿涅茨克和卢甘斯克宣布独立相关主题。此外，一些诱饵文档包含私人数据，这些数据为顿涅茨克和卢甘斯克两个国家内部工作流程的统计数据和文件。这个事实表明攻击者的目标是这两个地区的人民。ESETLiveGrid®遥测也证实了这些假设：在乌克兰，顿涅茨克和卢甘斯克是感染 Prikormka 恶意软件中最多的两个地区。

攻击者将电子邮件附件命名为具有挑衅或有吸引力的名字，利用社会工程学诱导受害者打开恶意附件。比如以下几个例子：

- Нацгвардейцы сошприцами сделали из донецкого мальчика мишень для ракет.exe（From the Russian: National Guard of Ukraine aimed rockets at boy from Donetsk）。 编译时间戳：2014 年 11 月 5 月
- Последнее обращение командира бригады 'Призрак' Мозгового Алексея Борисовича к солдатам и офицерам ДНР и ЛНР.scr(From the Russian: Leader of the Prizrak Brigade Aleksey Borisovich Mozgovoy'slast appeal to soldiers and officer of Donetsk From the Russian: Leader of the Prizrak Brigade Aleksey Borisovich Mozgovoy'slast appeal to soldiers and officer of Donetsk People’s Republic and Luhansk People’s epublic). 编译时间戳：2015 年 5 月 24 日
- Места дислокации ВСУ в зоне проведения ATO.scr (From the Russian: Dislocation of the armed forces of Ukraine in ATO zone). 编译时间戳：2015 年 12 月 15 日

这里有些用于攻击顿涅茨克和卢甘斯克分裂分子的诱骗文件示例：

The first example is an executable with the filename СПРАВОЧНИК по МИНИСТЕРСТВАМ обновленный.exe(From the Russian: Ministries directory – updated) that drops a decoy document with a list of Ministries of the self-proclaimed republic. The Campaign ID for this executable is D _ xxx. (Figure 3)

安全加社区 公益翻译项目 2016

СПРАВОЧНИК по МИНИСТЕРСТВАМ обновленный.exe(From the Russian: Ministries directory – updated)文件释放了一个包含自称为顿涅茨克共和国的部委名单的诱骗文件。（图 3）

• Here is another example of a decoy document, which was dropped by an executable named материалы к зачету по законодательству.exe(From the Russian: Materials for the law exam). This executable drops several documents including the LPR temporary constitution and other legal and political documents. The Campaign ID is L _ ment; the word “ment” is Russian slang for a policeman. Thus, the attackers demonstrate intimate knowledge of the Russian language. (Figure 4)

материалы к зачету по законодательству.exe(From the Russian: Materials for the law exam)可执行文件释放一些包含卢甘斯克的临时宪法和其他法律政治文件。活动 ID 为 L _ ment，“ment”为俄罗斯俚语中“警察”。因此，攻击者应为精通俄语的人。（图 4）

• Some of the decoy documents use the Minsk agreementtopic. Here is an example of one such document, which comes from a dropper with the filename Схема демилитаризованной зоны в районе Шиок ино.exe(From the Russian: Scheme of the demilitarized zone in the Shyrokyne(Shyrokyne written with a typo in Russian)). The Campaign ID was Lminfin. (Figure 5)

一些诱骗文件使用明斯克协议，比如 Схема демилитаризованной зоны в районе Шиок ино.exe(From the Russian: Scheme of the demilitarized zone in the Shyrokyne(Shyrokyne written with a typo in Russian)) dropper 的释放文件。活动 ID 为 Lminfin (图 5)

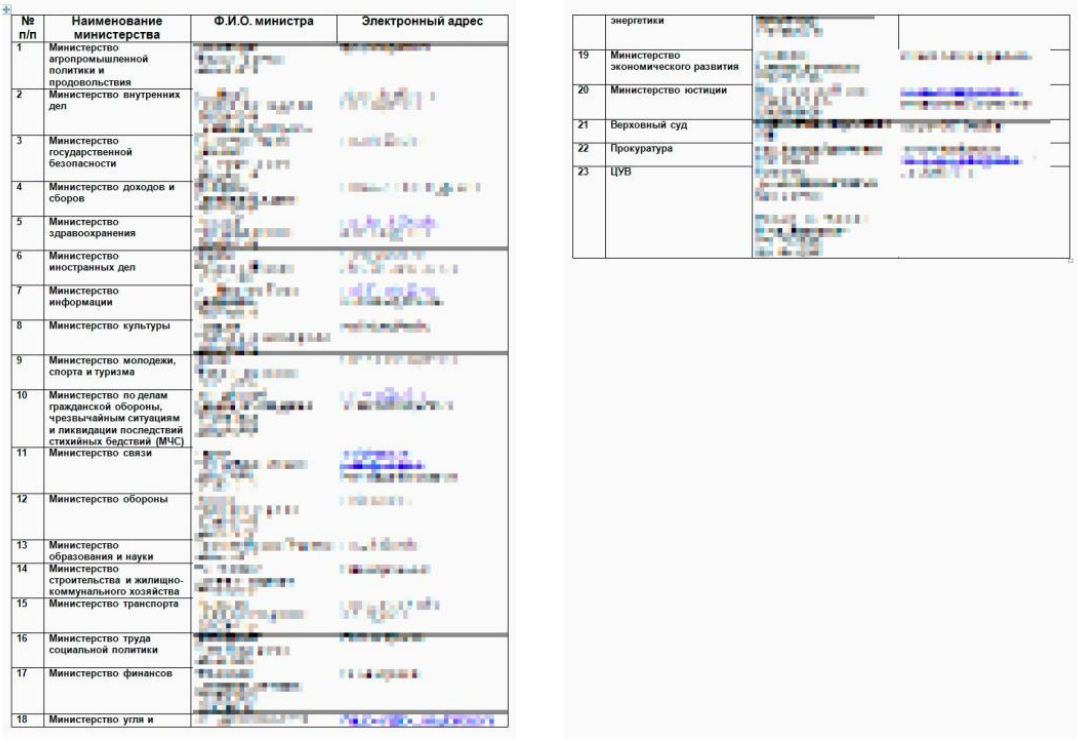
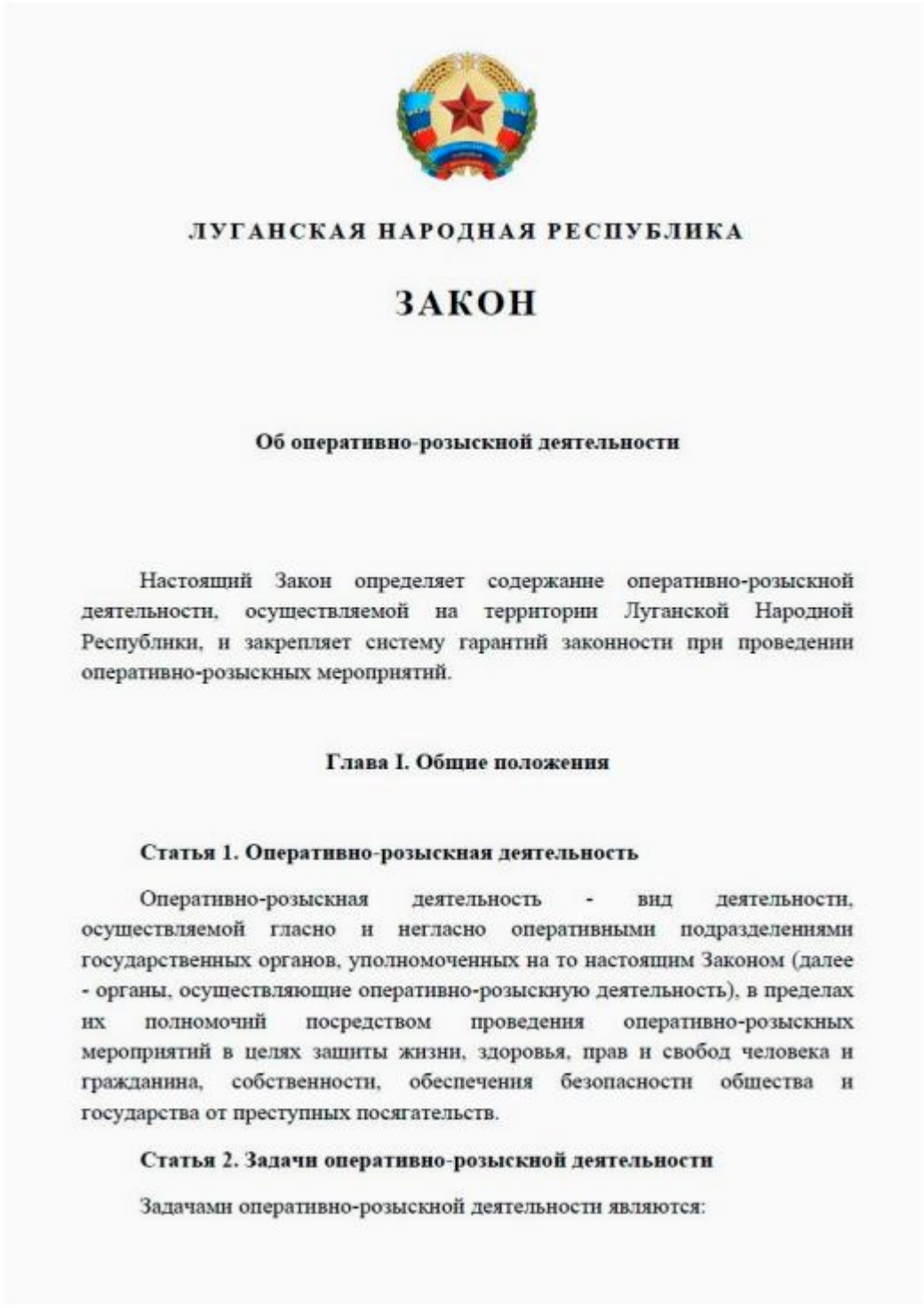


图 3 包含顿涅茨克部委名单的诱骗文件



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:

图 4 包含法律的诱骗文件，文件描述了特殊犯罪调查活动的规则

安全加社区
公益翻译项目
2016

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

图 5 诱骗文件，利用了明斯克协议主题

另一个诱骗文件包含了明斯克协议所建立的缓冲区地图。这也是一个示例，此诱骗文件来自Отвод с 4 участками по сост на 14.08.exe（From the Russian: Pullout [of heavy weapons] on 14.08），活动的 ID 为 BUR。

安全加社区
公益翻译项目
2016

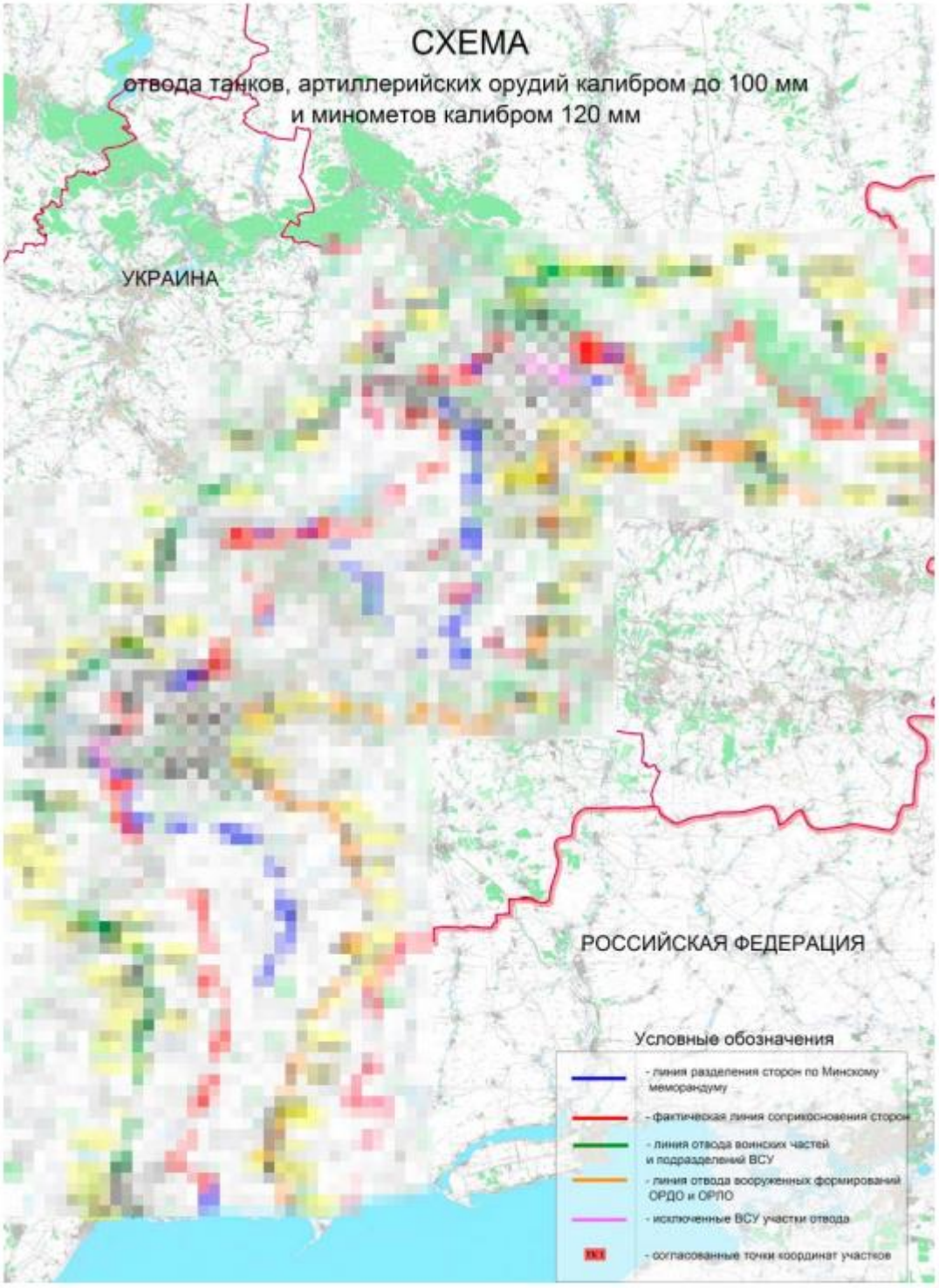


图 6 包含缓冲区的诱骗文件

重要提示：多数用于反对分裂主义的 Prikormka 二进制文件使用的活动 ID 以 D 或 L 为首字符，也就是说它分别表示顿涅茨克和卢甘斯克人民共和国。我们也观察到一个命名为Заявление Эдуарда Басаргина 13 октября 2015 года в 15 часов.exe(From the Russian: Eduard Basargin's statement on 13th October 2015 at 3pm)的执行文件使用的活动 ID 为 RF _ lgm。RF 前缀标明俄罗斯联邦，此结果已在俄罗斯证实。

安全加社区
公益翻译项目
2016

2.2 反对乌克兰民族的政党竞选活动

上述提及的诱骗文件，都是从包含俄语文件名的可执行文件中提取的。乌克兰语是国家官方语言，然而，东部乌克兰人倾向于使用俄语，而在西部，人们使用乌克兰语。

一些 Prikormka 二进制文件使用乌克兰语命名。比如，文件名П л а н ДН Р н а 21липня，щ о д о в і д в о д у в і й с ь к .exe（来自乌克兰：顿涅茨克人民共和国计划于 7 月 21 日撤军）。 使用乌克兰语作为的附件名表明，这种恶意信件接收者使用乌克兰语，而非俄语。 在乌克兰西部地区检测到 Prikormka 恶意软件的事实也加强了这一假设的正确性。这次活动的 ID 是 Psek，它表明 Prikormka 恶意软件将乌克兰民族党右翼成员作为攻击目标。

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

图 7 用于反对乌克兰民族党的诱骗文件

2.3 其他活动

Operation Groundbait 的目标不仅仅是顿涅茨克和卢甘斯克人民共和国分裂分子。研究过程中还发现其他有趣的诱骗文件，但是不能在这些文件的基础上确定目标受害者。

安全加社区
公益翻译项目
2016

命名为 Новое с л о в о жизни.exe(来自俄国：生命新篇章)的 dropper 释放出可能用于反对宗教学院的诱骗文件。活动 ID 为 medium，该活动 ID 可参考通灵与招魂。

图 8 用于反对宗教组织的诱骗文件

2016 年 3 月，出现了另外一场活动。此次活动的恶意文件名为匈牙利语：Önéletrajz fizikai munka 2.pdf.scr，翻译为英语为 CV physical work。此诱骗文件通过 Önéletrajz fizikai munka 2.pdf.scr 这个 dropper 释放，其文件内容为使用匈牙利语书写的个人简历。这种恶意的 scr 文件和其他两个文件（使用乌克兰语的个人简历、使用匈牙利语表示的能胜任此工作的证书）一起封装成压缩包格式发送，在这种情况下是很难确定攻击目标的，但是能够确定的是：收件人懂得乌克兰语和匈牙利语。这个序列的 ID 为 F_ego.

图 9 Prikormka 发送给受害者的匈牙利语文件

安全加社区
公益翻译项目
2016

通过 bitcoin.exe 释放诱骗文件，活动 ID 为 hmod。

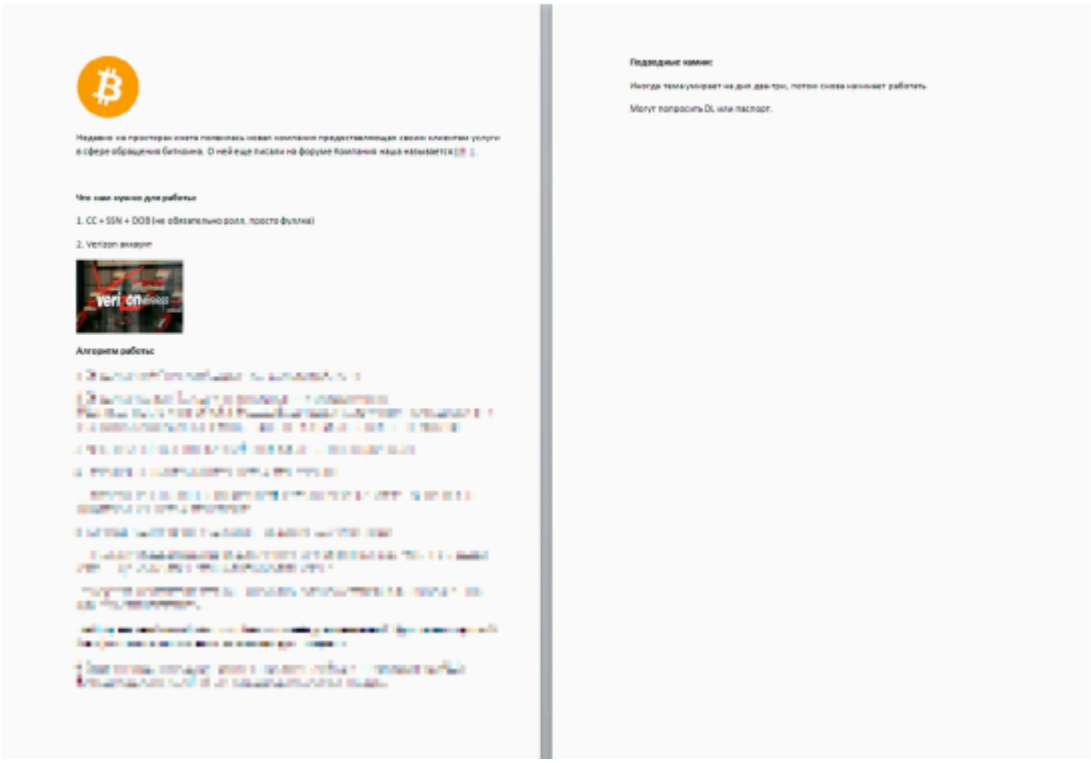


图 10 解释如何提交信用卡欺骗的诱骗文件

诱骗文件中的俄语文字解释了使用偷取的信用卡购买比特币的步骤，其中文件内容中包含的俚语（俄国领导通常使用）。

prikormka.exe 释放神秘的诱骗文件，活动 ID 为 30K _ alfa。

Официальный представитель "FIN" в Украине

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 $

安全加社区
公益翻译项目
2016

图 11 prikormka.exe 释放的神秘诱骗文件

这个诱骗文件包含一个乌克兰商店售卖的各种鱼饵价目表。

3 技术细节

本节从技术方面详细介绍了 Prikormka 恶意软件，包括软件架构、C&C（命令与控制）通信及对所使用模块的具体分析。

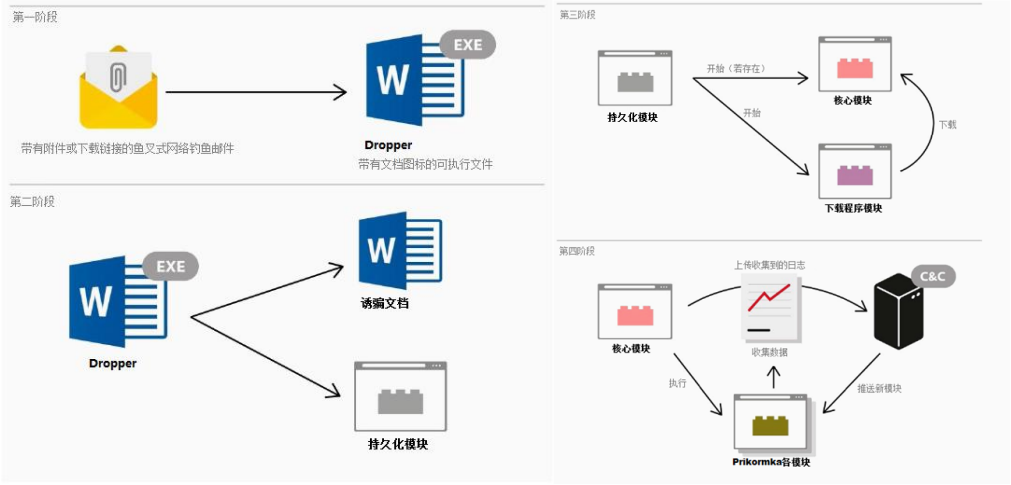


图 12 Prikormka 恶意软件架构简化方案

3.1 Dropper（病毒释放器）

Dropper 是这个恶意软件的初始组件，一般通过 email 附件发送。通常情况下，Dropper 的扩展名为.scr 或者.exe，被压缩为压缩文件格式。为了诱骗受害者，Prikormka Dropper 可以伪装成各种类型的文档或者自解压文件格式。

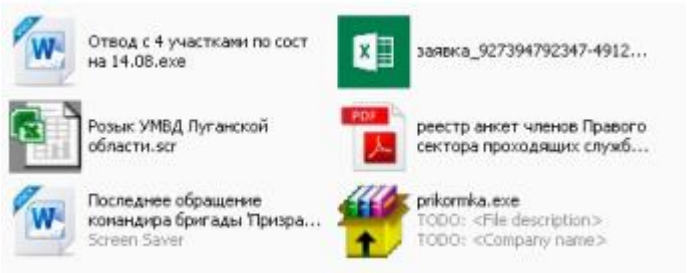


图 13 Prikormka 使用的图标

附件执行后，dropper 感染计算机，显示一个 WinRAR 自解压 （SFX）归档窗口提取出一个或多个诱骗文件。一些情况下，dropper 会创建并启动一个合法的无恶意的可执行文件。有趣的是，即使其 dropper 的文件名称使用的是乌克兰语，其自解压文件也会显示一个俄罗斯本地化的图形用户界面。若文件名是匈牙利语，Dropper 则根本不会呈现这个窗口。

安全加社区
公益翻译项目
2016

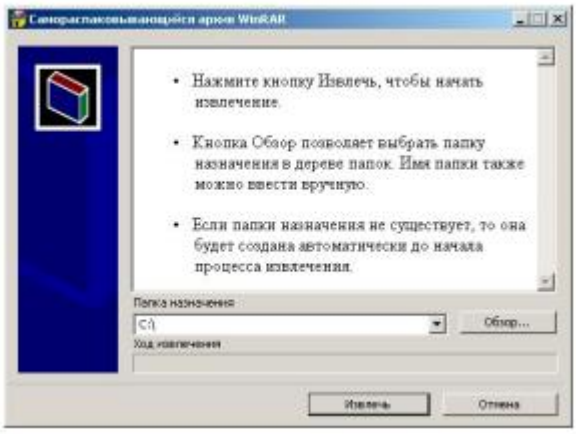


图 14 SFX 归档的俄语界面窗口

SFX 可执行文件包含一个或多个诱骗文档，比如，Prikormka 曾经释放了一个包含 24 个文档的 SFX 可执行文件。当然，诱骗文档的数量和大小会影响 Dropper 的大小，我们发现的最大 Dropper 其大小为 25 MB。

多数 Dropper 可执行程序具有一个嵌入式应用清单，规定可执行程序须有管理员权限才可在系统中运行。若用户没有管理员权限，系统会提示用户提供凭证。

```
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level="requireAdministrator" uiAccess="false"></requestedExecutionLevel>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>PADPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD
```

图 15 Prikormka dropper 中嵌入的应用程序清单

Dropper 之所以要求管理员权限是因为 Prikormka 使用的技术会永久存在于被感染系统。恶意软件使用 dll 劫持的目的是在系统每次重启时都能自动启动。通常情况下，dll 文件存储在 windows 目录下，在系统重启时，Windows 目录下的 dll 将会被 explorer.exe（资源管理器）进程加载，但 Dropper 在 windows 目录下保存一个 Prikormka dll 模块（命名为 ntshrui.dll），替代了原本的合法文件 C:\Windows\System32 \ntshrui.dll 被加载进资源管理器进程。这样 Prikormka 模块更改了 dll 文件的加载顺序，劫持了 dll 文件。这种攻击的方法已被杀软研究组织多次公开，并不算新颖。

Prikormka dropper 使用的另一个有趣的技术是使用.scr 格式文件，.scr 文件代表屏幕保护程序，是一个标准的 windows 可执行文件。.exe 和.scr 的主要区别在于屏幕保护程序由指定的命令行参数执行。通常情况下，网络犯罪只是使用.scr 扩展名重命名可执行文件从而绕过各种安全措施，但是 Prikormka 的作者实现了这种命令行参数检测，因此当二进制文件作为标准可执行程序执行时（不使用要求的参数），它不会感染系统。这种简单的检测使恶意软件能够绕过一些虚拟执行沙箱的分析。

使用.scr 文件感染系统的木马，使用标准方法（rundll32.exe）来加载恶意 dll，设置注册表的 key 来保证其一直存活(添加 key 的名称为 guidVGA 或 guidVSA)：
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run]
为了使 32 位/64 为 windows 资源管理器都能加载恶意软件，它包含了这两个平台的二进制文件。大多数模块使用 C++语言编写，使用 Microsoft Visual Studio 编译。

Dropper 在它的资源文件中存储模块，一些资源使用简单的 XOR 操作进行加密。

安全加社区
公益翻译项目
2016

图 16 Prikormka dropper 的二进制文件中包含的资源

Dropper 创建 rbcon.ini 文件，用于存储活动 ID 和其他数值。

早期的 Prikormka 版本使用与此不同的技术----活动 ID 内嵌于其中一个模块的二进制文件中。

图 17 嵌入二进制文件的活动 ID（值为 hmyr32）

编译时，将活动 ID 值硬编码在 Prikormka 的二进制文件中，适用于 32 位 os 版本的二进制文件中的 ID 以 2 结束，64 位版本的 ID 则以 4 结束。

在受害者数目较少的情况下，这种技术是有效的，然而一旦受害者的人数增加，它可能会给攻击者带来一些问题。为每个受害者重新编译和重新打包工具及核心部分将会花费很长时间，因此大约在 2015 年年中，攻击者改变了这个方案。从 2015 年 6 月起，活动 ID 存储在命名为 rbcon.ini 的单独的文件中，这个文件被攻击者称为对象集。恶意软件作者也增加了一个被称为 roboconid 的新值，这个值代表了使用者的 ID。通过调查可以确定此 ID 是恶意软件使用者的唯一标识码，恶意软件使用者可能使用此软件执行空间作战、分发感染、监控以及跟踪特定目标。

图 18 包含活动 ID 和使用者 ID 的 rbcon.ini 文件

一些 dropper 的二进制文件中包含 PDB 路径，通过这些路径可以发现攻击者使用的目录结构。

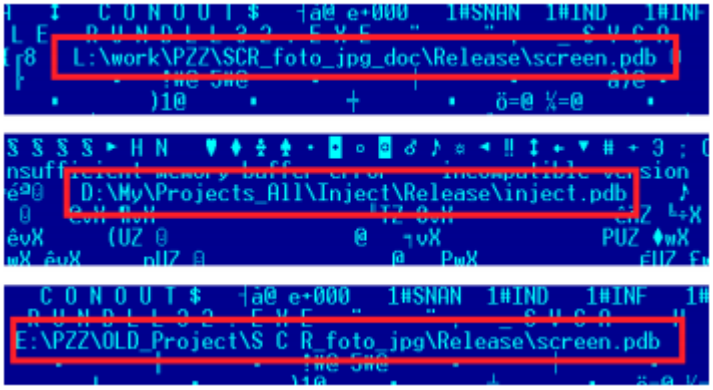


图 19 在 dropper 中发现一些 PDB 路径

恶意软件作者内部称此木马为 PZZ，我们还有其他证据能够支持这个结论。Prikormka 家族是一个典型的使用模块结构的网络间谍木马。这个木马的功能是从受感染计算机中窃取敏感信息并将其上传至 CC 服务器。

3.2 Prikormka 模块

该模块在受感染系统中以 dll 文件的形式存储，可实现多种功能，例如与 CC server 通信、辅助目的（如保证持续性）、泄漏受感染计算中包含的各种不同类型的敏感信息。之前提到过，Prikormka 模块支持 windows 32 位和 64 位两种平台。

下一节将详细介绍包含预定义名称的下载模块标准集。因此，为了执行模块（dll 文件），模块应该存储在特定的文件名下，并具有以下导出功能之一：启动，插入点（KickInPoint）、循环。攻击者可以将定制的模块推送至特定的受害者。目前观察到定制模块通常命名为 mp.dll.

应当注意的是，恶意软件使用者可以决定推送哪些模块到受感染的计算机。Prikormka 使用相似的名称存储不同功能的模块，相反的，也可以使用不同的名称存储相似功能的模块。一些恶意软件版本只存储当前日期和时间的模块名称。因此，下表中列出了插件的相关信息：

模块代码名称	内部模块名称	文件名	用途
PERSISTENCE	samlib.dll	samlib.dll，ntshrui.dll	持久化
DOWNLOADER	helpldr.dll	helpldr.dll，_wshdmi.dll	下载核心模块
CORE	hauthuid.dll	hauthuid.dll，_svga.dll,_wshdmi.dll	加载所有其他模块,与C&C服务器通信,上传日志
DOCS_STEALER	iomus.dll	iomus.dll	收集文档
KEYLOGGER	kl.dll，hlpuctf.dll	hlpuctf.dll	键盘记录
SCREENSHOTS	scrsh.dll	scrsh.dll	屏幕截图

安全加社区 公益翻译项目 2016

MICROPHONE	snm.dll	snm.dll	抓取麦克风音频
SKYPE	swma.dll	swma.dll	记录Skype音频电话
LOGS_ENCRYPTER	atiml.dll	atiml.dll	压缩、加密收集到的日志
GEOLOCATION	geo.exe	Inv.exe	定位受感染计算机
OS_INFO	InfoOS	mp.dll	收集受感染计算机的信息
PASSWORDS	Brother	mp.dll	收集各种已安装应用的密码
FILE_TREE	mpTREE	mp.dll	收集受感染计算机固定磁盘的文件目录树

表 1 Prikormka 模块标识列表

以下列表包含恶意软件代码所涉及的模块名称，但是由于我们在研究过程中没有看到过他们，因此无法评估其功能。

- miron.dll
- meta.dll
- h muid.dll
- sh.exe
- mupdate.exe

需要注意的是在 2008-2010 年间产生的 Prikormka 旧组件使用了完全不同的命名方案，以下是一些示例：

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

3.3 持续性模块（PERSISTENCE module）

如上所述，本模块使用 DLL 加载顺序劫持技术在系统中维持持久化。

当启动时，这个模块创建文件夹%USERPROFILE%\AppData\Local\MMC，并从%WINDIR%目录下拷贝以下文件：

- hauthuid.dll (CORE)
- hlpuctf.dll (KEYLOGGER)
- atiml.dll (LOGS _ ENCRYPTER)
- iomus.dll (DOCS _ STEALER)

安全加社区 公益翻译项目 2016

- swma.dll (SKYPE)
- helpldr.dll (DOWNLOADER)
- rbcon.ini

该组件查找并执行 CORE 模块，如果未找到 CORE 模块，则执行 DOWNLOAD 模块。

如果%USERPROFILE%\AppData\Local\MMC\nullstate.cfg 文件存在，则组件从 MMC 目录下删除上述所列的所有文件并退出，对自己做了去激活操作。

一些 PERSISTENCE 模块中包含 PDB 路径，这个路径可以解释恶意软件作者在编译时使用的目录结构。图 20 中，三个 PDB 路径包含一个时间戳，可能为项目创建或更改时间。其中某个 PDB 路径包含俄文字符串 Ｐａб.Программы，可被翻译为“办公用计算机程序程序”。

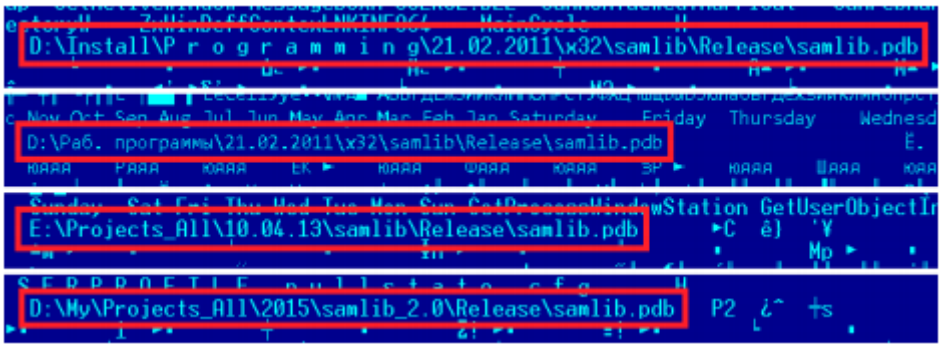


图 20 部分 PERSISTENCE 模块中发现的 pdb 路径

3.4 下载模块（DOWNLOADER module）

该模块负责下载并执行核心模块。向其中一个 C&C 服务器发送 HTTP 请求后，模块从服务器收到数据并对其解密，然后将数据保存在名为 hauthuid.dll 的文件中，最后加载该文件。这一通信过程采用 Blowfish 加密和 Base64 编码。

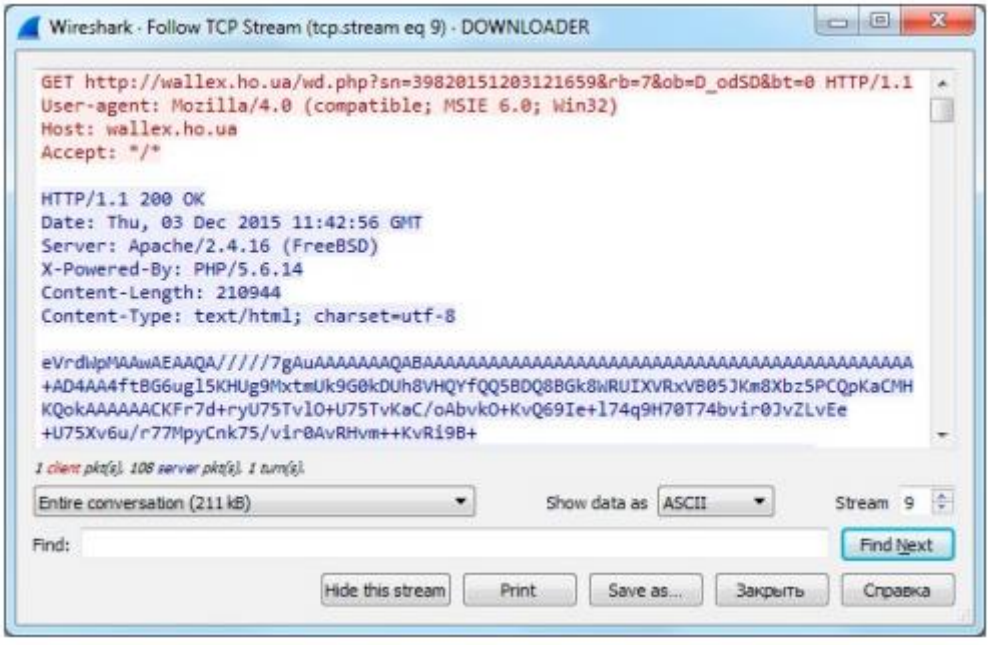


图 21 Prikormka 恶意软件中 DOWNLOADER 模块中捕获的流量

该模块包含活动 ID、使用者 ID 、受感染的日期和时间、操作系统平台（32 位/64 位）。一些 DOWNLOADER 模块的二进制文件中包含 PDB 路径，表明在攻击者内部，此模块被称为 Loader 或 helpldr。

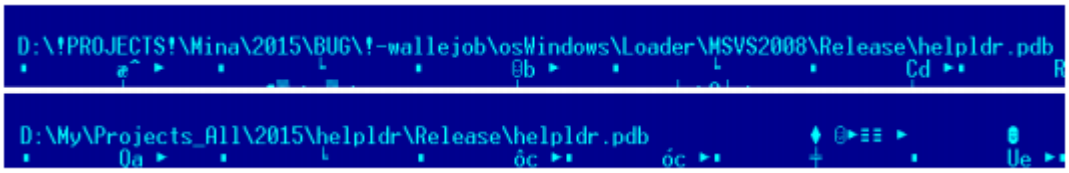


图 22 DOWNLOADER 模块中发现的 PDB 路径

3.5 核心模块（CORE module）

核心模块负责与C&C服务器进行通信并执行以下任务：下载并加载其他模块，并将盗取的数据上传到远程服务器。

Prikormka（尤其是核心模块）已有几年历史，其实现细节可能不尽相同，但其核心模块的基本原理却从未有过变动。该恶意软件的实现原理很简单： 核心模块下载其他组件用于获取各类数据。此类模块加载后，将收集敏感数据，并将这些数据以明文或加密的方式保存在特定日志文件中。核心模块会定期查看是否有新日志生成，如果有，将日志上传至远程服务器。核心模块最大可上传500 MB的日志文件。

该模块创建以下两个目录存储可供下载的模块和所收集的日志文件：

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

MMC文件夹存储其他可供下载的恶意软件组件。SKC文件夹存储所收集的日志文件。下文用“日志文件夹”指代SKC目录。

这些可供下载的模块无法上传所收集的数据。事实上，只有核心模块和下载程序模块可以与 C&C 服务器通信。并且，这两个模块采用相似的通信协议。

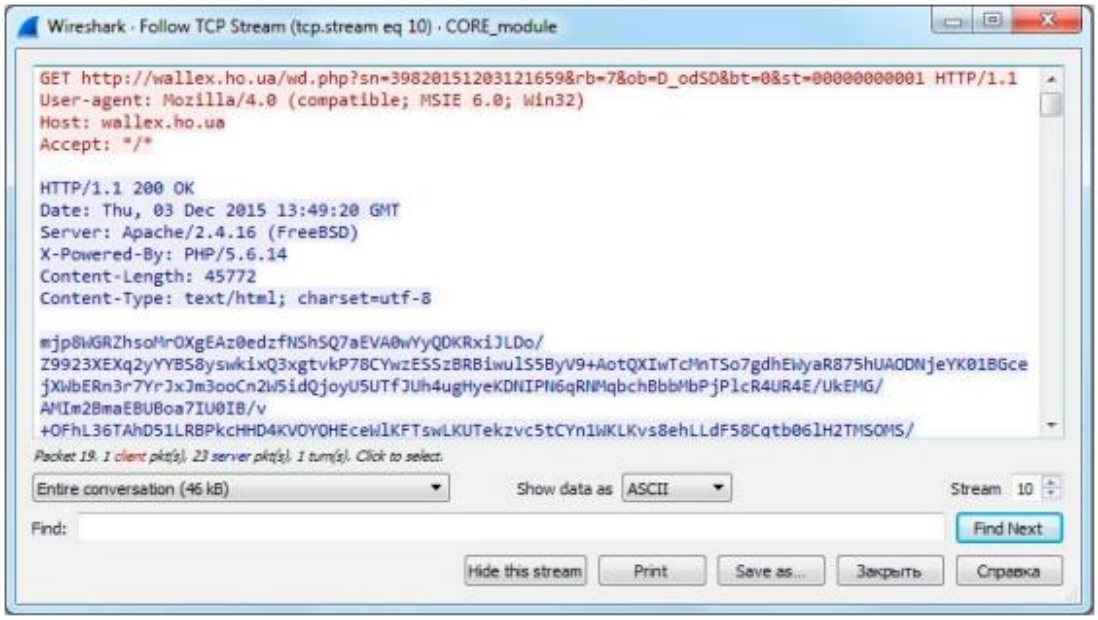


图 23 Prikormka 恶意软件中 CORE 模块中捕获的流量

这两个模块发送的HTTP请求大致相同，唯一区别是其URL中包含的st参数。该参数表明哪些可供下载的模块处于激活状态且已被Prikormka加载。目前来看，该恶意软件还可加载11个这样的模块。收到请求后，服务器器返回需执行的模块的名称或空内容。

核心模块使用下列相似的 URL 发送 POST 请求进行日志上传：

- http:/server.ua/wd.php?sn=%DATE _ TIME _ OF _ INFECTION%

需要注意的是，早期版本的 Prikormka 以明文形式存储 C&C 服务器。后来，为了隐藏服务器的地址，攻击者采用 Base64 算法存储服务器。最新版本的核心模块采用了简单加密。解密时，研究人员需在每个加密的字节中添加十六进制的值 0x17。

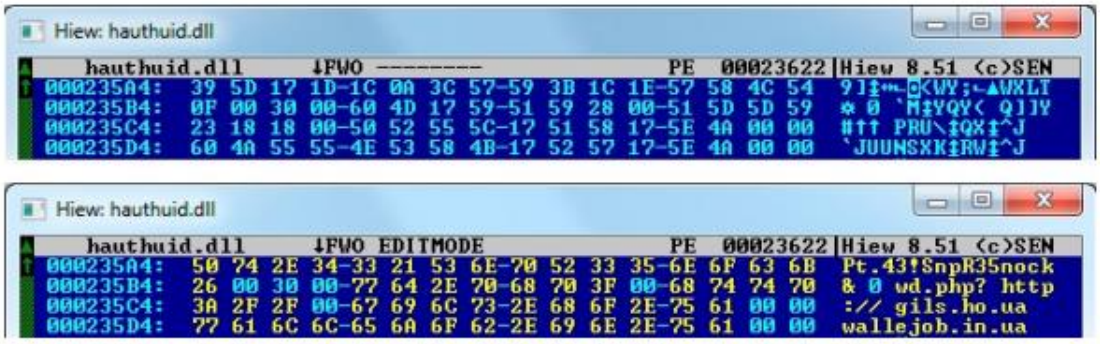


图 24 Prikormka 使用简单的加密算法隐藏 CC server

3.6 文件窃取模块（DOCS_STEALER module）

该模块负责从固定硬盘或通过 USB 口连接的移动媒介中收集文档。

该模块主要收集具有以下扩展名的文件：.doc、.xls、.docx、.xlsx、.ppt、.pptx、.pps、.ppsx、.pdf、.txt 和.odt。不过，该模块只收集最近 7 天（或 14 天或 30 天，时间因模块版本而异）修改的带有以上扩展名的文件。

收集后，该模块对这些文件进行压缩、利用 Blowfish 加密，之后将其保存在名称为以下格式的文件中：

- %USERPROFILE%\AppData\Local\ioctl\%DISK _ ID%\%DATE% _ %TIME%.kf

3.7 密码记录模块（KEYLOGGER module）

该模块用于收集键盘输入和最前显示的窗口标题。收集的信息存储在日志文件夹中，文件名为：

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

如果日志文件超过 10M，此模块将移除日志并重新开始，一些版本中的模块使用 Blowfish 算法加密日志文件。

安全加社区 公益翻译项目 2016

3.8 屏幕截图模块（SCREENSHOTS module）

该模块负责截取受害者桌面图像。

默认每 15 分钟截图一次。但如果受害者打开了 VoIP 应用如 Skype 或 Viber，截图间隔降至 5 秒。截图以 JPEG 格式保存在日志文件夹中，文件名为%DATE% _ %TIME%.tgz.scrsh 或%DATE% _ %TIME%.stgz。

3.9 麦克风模块（MICROPHONE module）

该模块负责录制来自麦克风的声音。它可录制10分钟的音频。如收到停止录制命令或空间不足时，该模块停止录制。所录制的音频由LAME MP3编码器进行编码，保存在日志文件夹中，文件名为filename %date% %TiME%.snm。

3.10 SKYPE 模块（SKYPE module）

该模块负责录制Skype上的音频聊天。为录制Skype上的呼叫，该模块使用称为Skype桌面API的合法接口。若第三方应用使用此接口，Skype将弹出警告，由用户决定是否允许其接入。为了绕过Skype的这一安全特性，Prikormka模块创建了一条线程，以定位警告窗口并自动单击“允许接入”（Allow access）按钮，而无需手动操作。

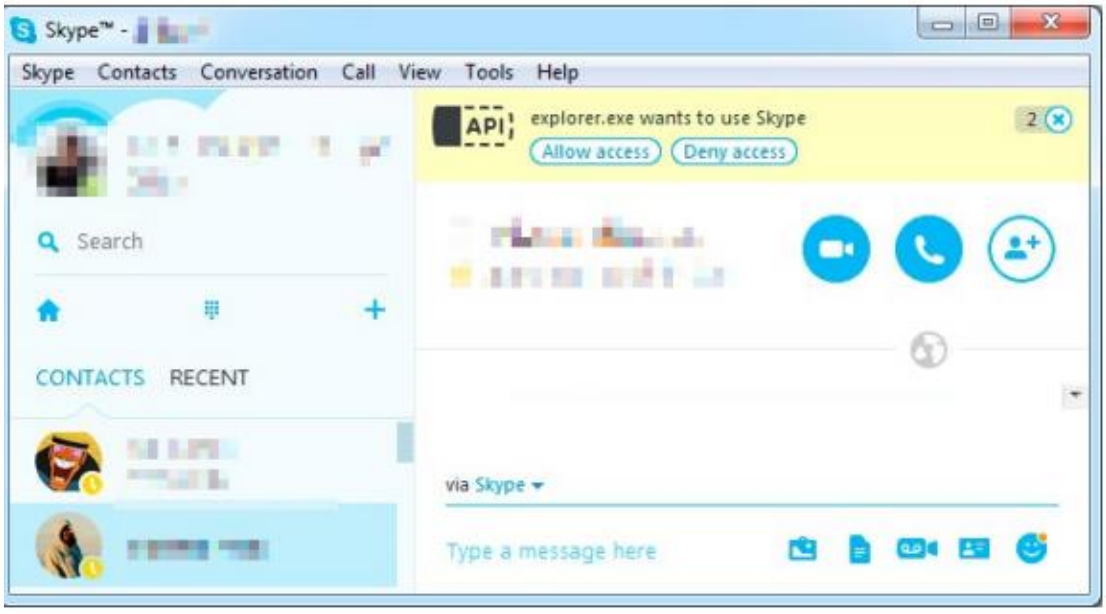


图 25 skype 显示警告

在通过该模块的某些字符串和代码段可以看出，这个模块在一定程度上借鉴了 openrce.org in 2006 网站上发布的代码。

```
.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
```

图 26 字符串“CREATE APPLICATION minishell”标明“复制粘贴”的代码

该模块所录制的信息保存在日志文件夹中，文件名为%date% _ %TiME%.skw and _ skype.log。

3.11 日志加密模块（LOGS_ENCRYPTER module）

此模块用于日志加密。此模块通过 LZSS 算法压缩数据，并使用 Blowfish 算法加密以下日志文件：

- %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
- Files listed in %USERPROFILE%\AppData\Local\MMC\ierdir.dat

ierdir.dat 由核心模块创建。该文件中包含一份加密清单，列举了攻击者要从受害人的计算机中请求的文件。

加密后，未加密原文件（未加密）将被删除。加密文件将被存放在以下文件中：

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

另外，加密文件通过 Base64 算法编码。有趣的是，该模块将在加密文件的内容前添加以下特征：

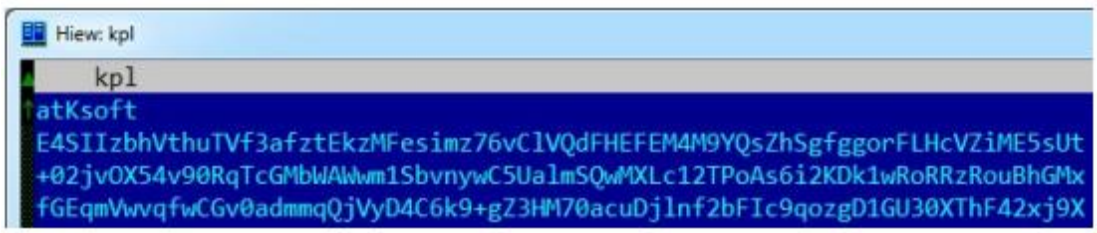


图 27 加密日志文件文件起始处的 atKsoft 签名

目前还没有找到任何能够读取此文件的合法应用程序，也未找到其他与 atKsoft 相关的数字签名含义。

3.12 地理定位模块（GEOLOCATION module）

该模块负责收集感染此恶意软件的计算机的地理信息，以便对其进行定位。该模块与其他模块不同的一点是它基于C#语言。该模块收集当前可接入的WiFi网络相关信息，包括服务集标识（SSID）和MAC地址。之后，该模块请求Google服务，将所收集的信息作为参数提供。基于此信息，Google的服务响应返回可能的地理位置。

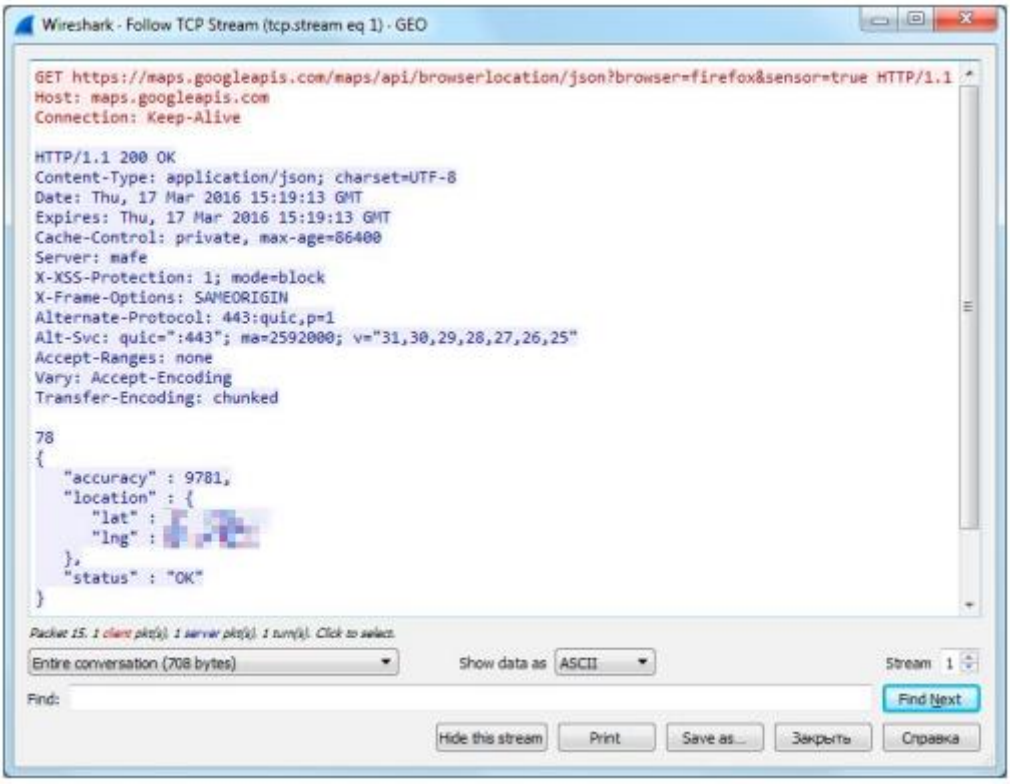


图 28 地理定位模块通信数据包

收集到的地理位置信息保存在日志记录目录下的 geo%DATE%.inf 文件中。

图 29 地理位置定位模块包含的 pdb 路径信息

3.13 系统信息收集模块（OS_INFO module）

该模块负责收集关于被感染计算机的信息，包括：

- 笔记本电源信息
- Windows 系统版本
- 计算机名和用户名
- IP 地址和 MAC 地址
- 内存
- 可用磁盘

- 可用打印机
- 屏幕分辨率
- 安装杀毒软件情况

该模块使用 Windows 系统 API 收集信息，收集到的系统信息保存在日志记录目录下的%DATE%_%TIME%.inf 文件中。

3.14 密码收集模块（PASSWORDS module）

该模块用于收集受感染系统上存储的应用程序密码数据。
该模块收集以下软件中保留的用户名密码信息：

- 谷歌 Chrome 浏览器
- Opera 浏览器
- Yandex 浏览器
- 科摩多龙安全浏览器
- Rambler 浏览器（Nichrome）
- 火狐浏览器
- 雷鸟浏览器

出于被检测的原因，该模块不收集微软 IE 浏览器和 Edge 浏览器上的密码信息。由于 Yandex 浏览器和 Rambler 浏览器主要在讲俄语的国家很受欢迎，我们认为此模块正是为了攻击这些国家的用户而设计的。
收集的信息保存在日志文件夹中，文件名为 %DATE% %TIME%.inf。

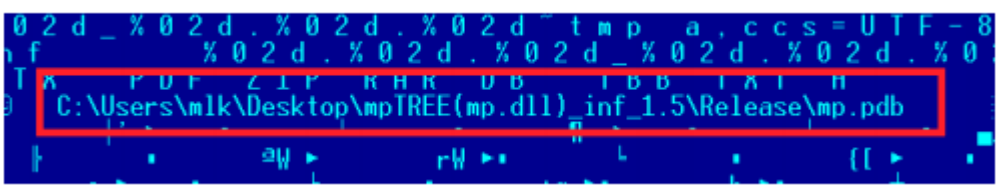
3.15 文件浏览模块（FILE_TREE module）

该模块负责收集计算机固定驱动器的文件系统信息，包括特定扩展名的文件的路径、大小和创建时间。该模块并不收集文件中包含的具体内容。

攻击者收集的文件类型信息：

Documents: TXT, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF
Archives: ZIP, RAR
Databases: DB, SQLITE
The Bat! email client: TBB, CFG, CFN, TBN, TBB
Microsoft Outlook: OST, PST
Other: DAT, WAV, EXE

Bat 邮件客户端软件在俄语系的国家中比较普遍，事实上该恶意软件的攻击目标主要是使用俄语系的计算机用户。
收集到的信息保存在日志记录目录下的%DATE%_%TIME%_tree.inf 文件中；其中某些模块中包含 PDB 路径信息，下图泄漏了恶意软件作者的用户名信息：



安全加社区 公益翻译项目 2016

图 30 文件浏览模块-PDB 路径泄露

4 C&C 服务器

在研究过程中，我们发现大部分服务器域名和地址都在乌克兰，并由该国的托管服务商托管。附录 B 中包含了更全面的列表信息。

根据托管公司的信息，其中一个 C&C 服务器 gils.ho.ua，自 2008 年以来一直在运营中。为了掩盖其非法活动，攻击者创建了一个虚假网站，专门针对乌克兰的首都—基辅。

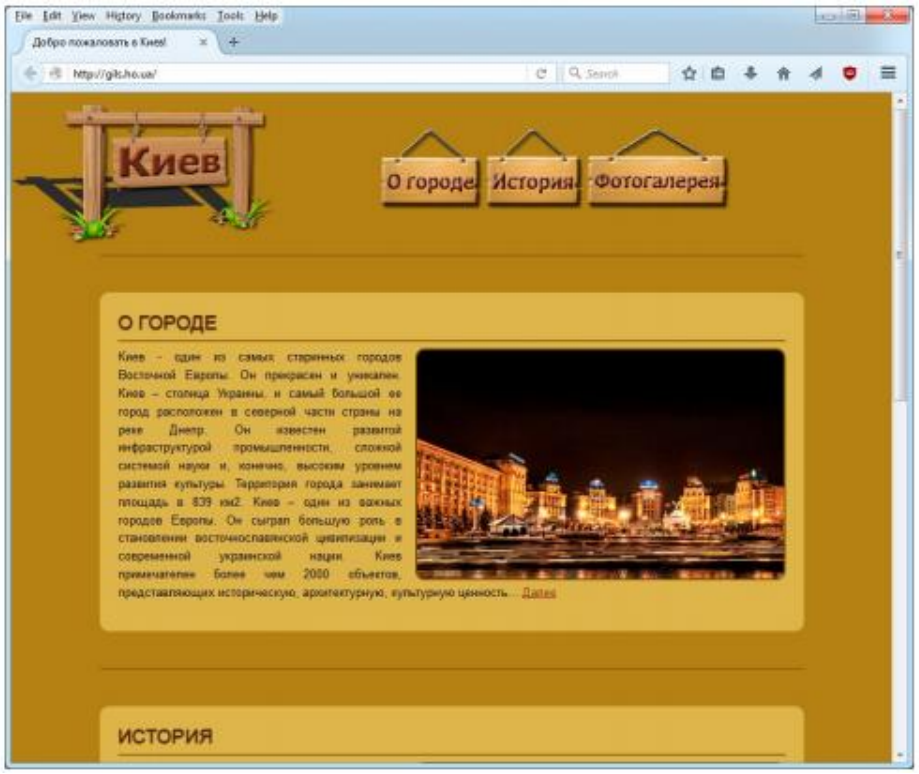


图 31 攻击者创建网站

调查过程中，我们访问了 Operation Groundbait 的一个 C&C 服务器。该服务器配置不当，允许我们查看公共目录列表。

安全加社区
公益翻译项目
2016

图 32 C&C 服务器目录列举

图 33 子目录内容

根目录包括33个子目录，其中的每个文件夹针对一个特定的受害者。这意味着服务器被用来控制33台感染Prikormka的计算机。子文件夹的名称包括操作员ID、活动ID和受感染设备架构。

每个文件夹包括2个名为data和util的子文件夹data文件夹包含泄露的加密数据，util文件夹包含加密的Prikormka模块。

除了data和util文件夹之外，针对特定受害者的子文件夹还包括2个格式的日志文件：journal 和log。有趣的是，这两个日志文件中竟然列出了恶意软件操作员和其他受害者。

log文件包含服务器和受感染计算机之间的通讯日志，具体为感染计算机的IP地址、日期和时间、请求类型（GET或POST请求）、请求大小，以及Prikormka模块的状态（如果是GET请求的话）。

安全加社区
公益翻译项目
2016

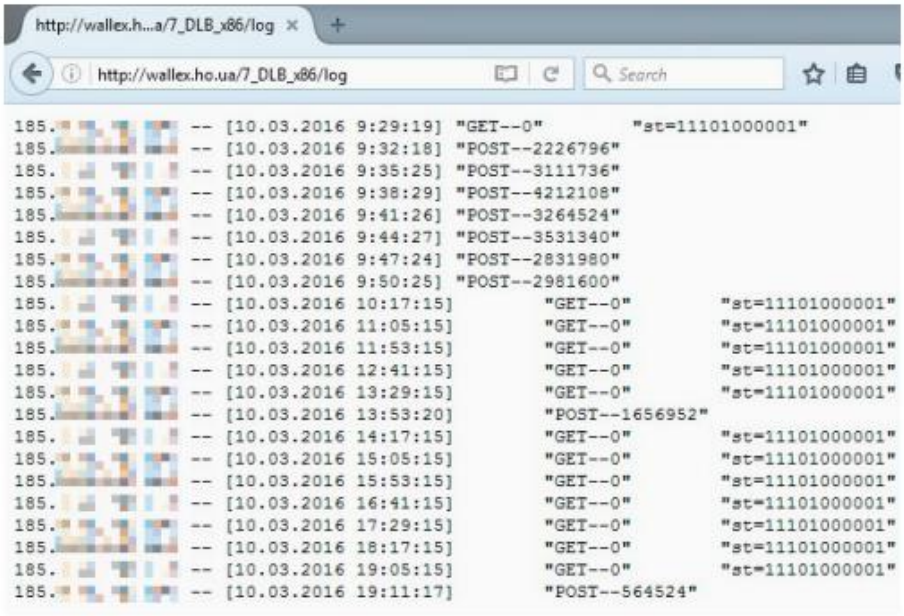


图 34 Operation Groundbait C&C 服务器上的 log 文件内容

journal文件包含服务器和恶意软件操作员之间的通信日志，具体为操作员IP地址、日期、时间和请求类型。值得注意的是，一旦恶意软件操作员下载了journal文件，文件（连同泄露的数据）都将从服务器上移除。

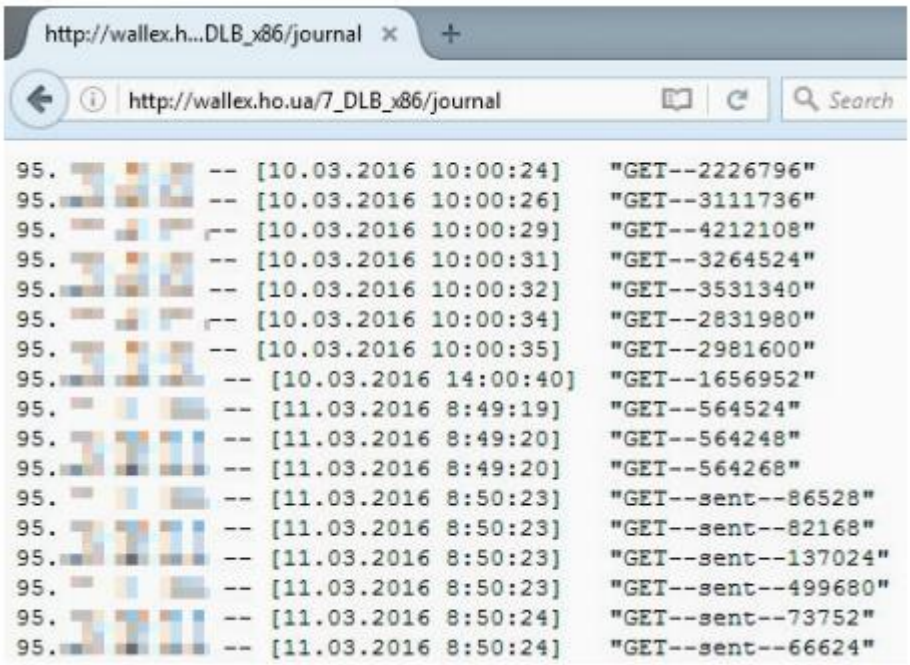


图 35 Operation Groundbait C&C 服务器上的 journal 文件内容

通过对一个包含 33 个受害者的 c&c 服务器上的通信日志分析，可以确认大多数受感染主机位于乌克兰东部，除此之外，还有一些受害者位于俄罗斯、乌克兰基辅；

日志的分析表明，恶意软件使用者通过使用 Kiev 和 Mariupol 的不同互联网服务提供商连接至服务器，其中一些还通过 Tor 网络访问 C&C 服务器。

安全加社区
公益翻译项目
2016

5 溯源（Attribution）

在这一节中，我们通过攻击者故意或无意中留下的线索，尝试寻找攻击的来源；

- 大多数 Prikormka 的 C&C 服务器位于乌克兰，并由该国托管公司托管
- 这一威胁背后的团队掌握了流利俄罗斯和乌克兰语。这一点可在诱骗文档和和恶意软件的二进制文件得到印证。
- 有些 PDB 路径泄露攻击者使用的俄文目录名。
- 在所有已分析的 Prikormka dropper 中，其 PE 资源中都包含与乌克兰或俄国相关的语言代码(乌克兰 0x0422，俄国 0x0419，如图 36 所示)。

图 36 dropper 的语言代码分布

Prikormka 的二进制文件编译时间戳表明此恶意软件作者使用了东欧时区的时间。

C&C 服务器日志表明，一些参与 Operation Groundbait 的恶意软件操作者已通过基辅和马里乌波尔的互联网服务提供商，获得连接。

有趣的是，早期的 dropper（2012-2015）确实包含俄语语言代码资源，在 2015 年中期，恶意软件作者开始逐渐从俄语转换为乌克兰语。

图 37 为 Prikormka 样本编译时间(小时)统计。

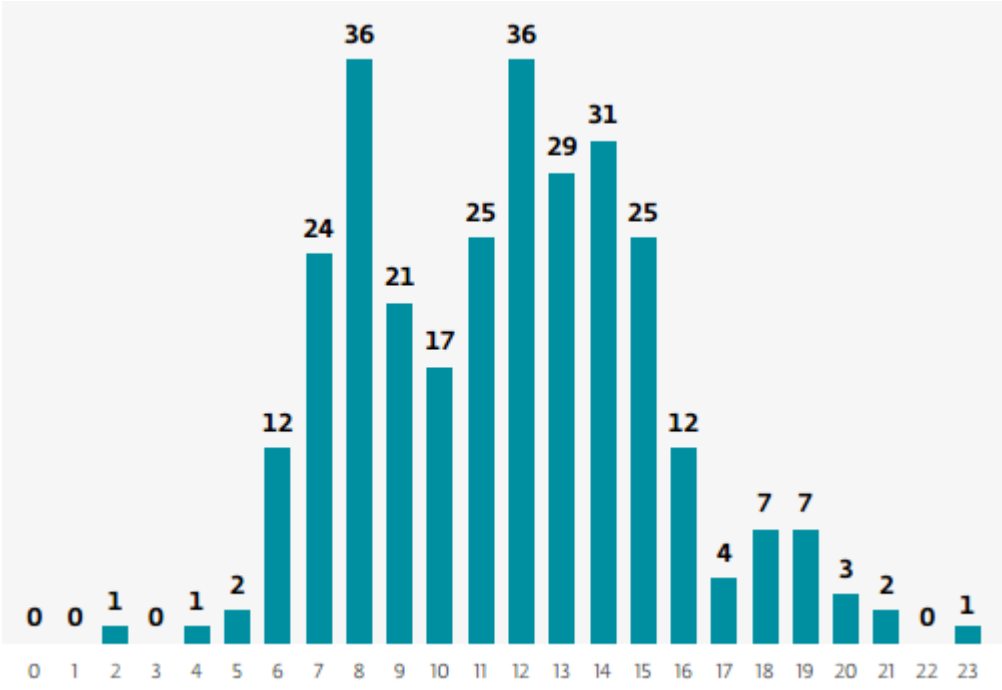


图 37 样本编译时间统计（UTC）

安全加社区
公益翻译项目
2016

我们可以推断出，恶意软件作者的工作时间是6:00–16:00（UTC），有时晚上会熬到很晚。这对应东欧时间8:00–18:00，恰恰是乌克兰的正常工作时间。

基于研究和上述事实，我们认为Operation Groundbait背后的攻击者倾向于监控或监视顿涅茨克和卢甘斯克地区的分裂主义分子或某些引人注目的目标，包括乌克兰政治家。恶意软件操作者和/或作者都懂乌克兰语和俄罗斯语，并有可能在乌克兰边境内操作。

6 结论

我们对这些攻击活动以及 Prikormka 恶意软件的研究表明，此恶意软件家族威胁是首次公开的用于特定目标攻击的乌克兰恶意软件。在技术先进性方面而言，攻击者没有使用任何复杂方法或新技术。但是攻击者是否使用了新技术并不重要，重要的是他们能够达到最终目的：从目标计算中窃取他们所需要的敏感信息。

在Operation Groundbait背后，攻击者取得的最显著成绩是他们活动长达7年之久，却从未被发现。至少2008年以来，恶意软件已进入大众视野。二进制文件时间戳、ESET遥测和所涉及的服务提供商都能够证实这一点。

继 BlackEnergy 和 Operation Potao Express 之后， Groundbait Operation 又一次证明：在武装冲突中使用具有高度针对性的间谍软件已成为日常现实。

在附录 B 或 github 中的 IOC 可用于标识感染信息。

安全加社区
公益翻译项目
2016

7 附录 A PriKormka 细节

PT Time stamp (UTC)	Campaign ID	Malware Operator ID
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	lff	N/A
Dec 01 08:07:07 2014	hmyr3	N/A
Dec 05 13:11:35 2014	lll	N/A
Jan 31 13:19:22 2015	lvo	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

PT Time stamp (UTC)	Campaign ID	Malware Operator ID
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	zkoniv	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

PT Time stamp (UTC)	Campaign ID	Malware Operator ID
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_mini	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_leco	7
Feb 05 08:20:01 2016	MM_lkur	7
Feb 05 08:51:46 2016	L_lml	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

PT Time stamp (UTC)	Campaign ID	Malware Operator ID
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

安全加社区
公益翻译项目
2016

8 附录 B Indicators of Compromise (IoC)

可以通过如下 IOC 集成提升检测与防护能力:
https://github.com/eset/malware-ioc/tree/master/groundbait

安全加社区
公益翻译项目
2016

安全加社区

公益翻译项目

2016

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。