Bisonal恶意软件变种分析

angel010 / 2018-08-03 01:00:53 / 浏览数 2577 技术文章 技术文章 顶(0) 踩(0)

本文翻译自：https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea/

攻击概要

5月初，Unit
42的研究人员发现一起针对俄罗斯国防公司和韩国企业的攻击活动，攻击活动中传播的恶意软件是Bisonal恶意软件的变种。Bisonal恶意软件从2014年就开始活跃了。Biso

截止目前，研究人员只收集到该变种的14个样本，说明使用并不广泛。在攻击活动中，攻击者会诱使用户加载伪装为PDF文件的Windows可执行恶意软件。下面对针对俄罗

针对俄罗斯的攻击活动

研究人员发现针对俄罗斯的攻击活动主要目标为提供通信安全服务和产品的公司，这些被攻击企业的另外一个特点是提供加密和密码服务，并开发了包括电信系统和数据保护

图1是发给目标企业的鱼叉式钓鱼攻击的邮件，邮件伪装成来自于俄罗斯工业与科技集团(Rostec)，Rostec主要致力于研发、生产及出口高科技产品。

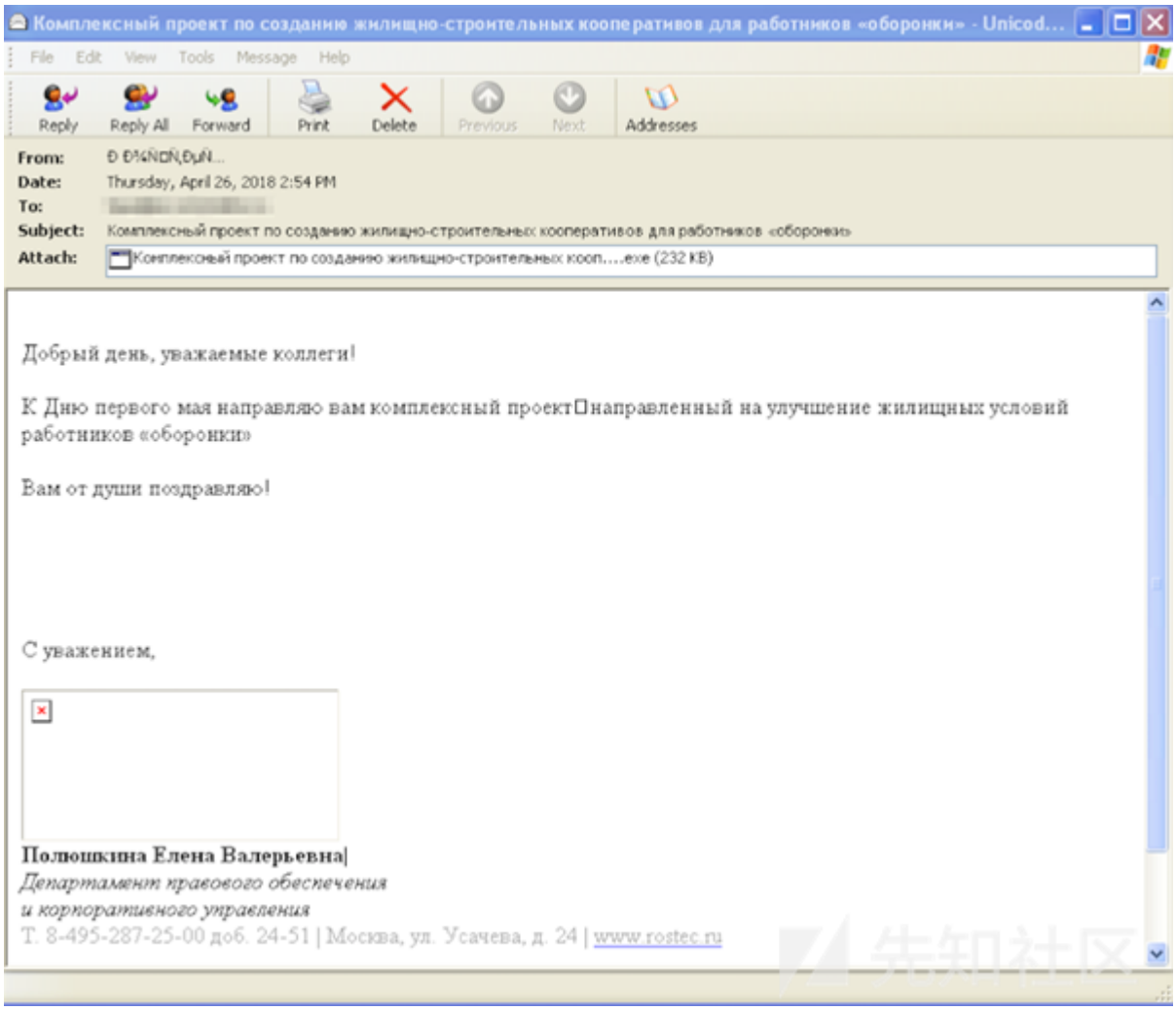
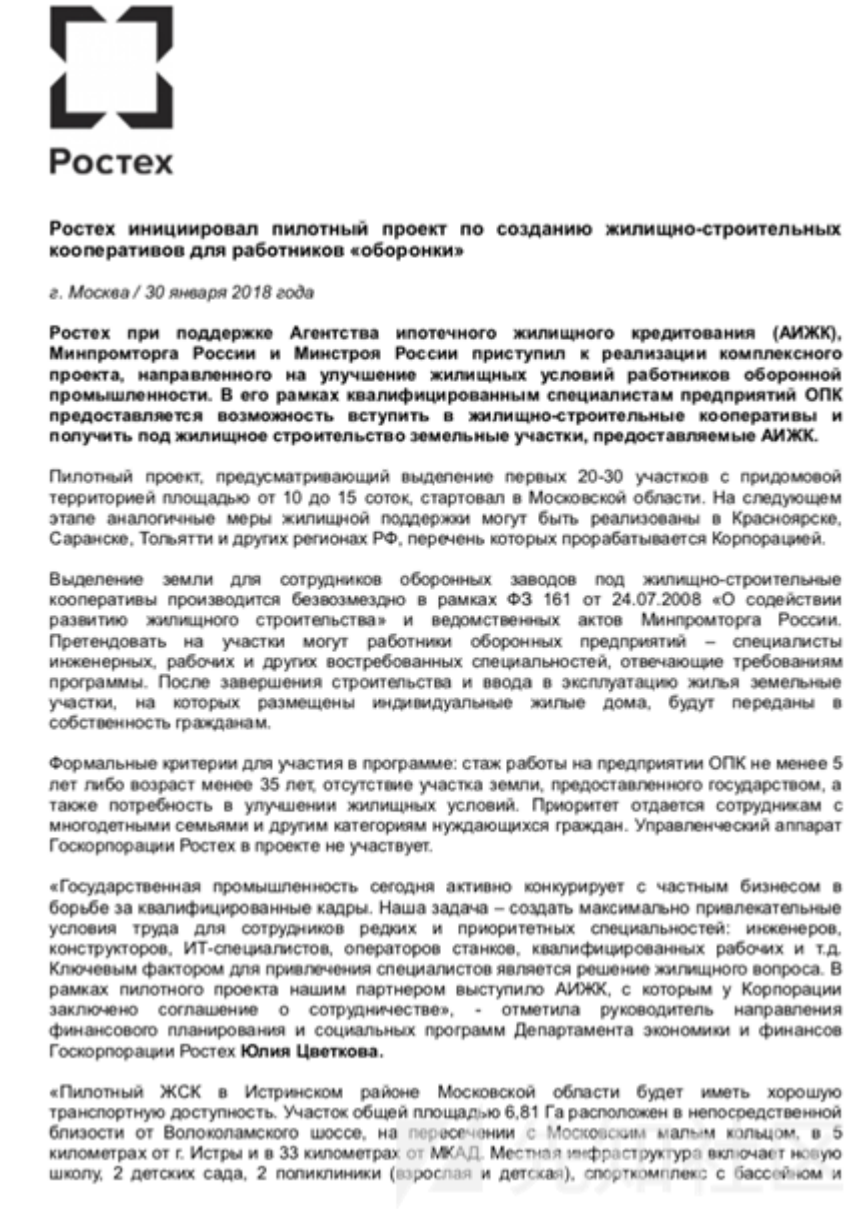


图1. 发给俄罗斯公司公司的鱼叉式钓鱼邮件

邮件的大致内容为该公司中标了"国防工程住房建设合作社综合项目"，并含有一个exe附件。

如图1所示，一些客户端软件并不会把附件显示为pdf文件。但把文件保存到电脑后，就会显示为pdf文件。一旦恶意可执行附件打开，主payload就会释放到受害者设备上，



Ростех

Ростех инициировал пилотный проект по созданию жилищно-строительных кооперативов для работников «оборонки»

г. Москва / 30 января 2018 года

Ростех при поддержке Агентства ипотечного жилищного кредитования (АИЖК), Минпромторга России и Минстроя России приступил к реализации комплексного проекта, направленного на улучшение жилищных условий работников оборонной промышленности. В его рамках квалифицированным специалистам предприятий ОПК предоставляется возможность вступить в жилищно-строительные кооперативы и получить под жилищное строительство земельные участки, предоставляемые АИЖК.

Пилотный проект, предусматривающий выделение первых 20-30 участков с придомовой территорией площадью от 10 до 15 соток, стартовал в Московской области. На следующем этапе аналогичные меры жилищной поддержки могут быть реализованы в Красноярске, Саранске, Тольятти и других регионах РФ, перечень которых прорабатывается Корпорацией.

Выделение земли для сотрудников оборонных заводов под жилищно-строительные кооперативы производится безвозмездно в рамках ФЗ 161 от 24.07.2008 «О содействии развитию жилищного строительства» и ведомственных актов Минпромторга России. Претендовать на участки могут работники оборонных предприятий – специалисты инженерных, рабочих и других востребованных специальностей, отвечающие требованиям программы. После завершения строительства и ввода в эксплуатацию жилья земельные участки, на которых размещены индивидуальные жилые дома, будут переданы в собственность гражданам.

Формальные критерии для участия в программе: стаж работы на предприятии ОПК не менее 5 лет либо возраст менее 35 лет, отсутствие участка земли, предоставленного государством, а также потребность в улучшении жилищных условий. Приоритет отдается сотрудникам с многодетными семьями и другим категориям нуждающихся граждан. Управленческий аппарат Госкорпорации Ростех в проекте не участвует.

«Государственная промышленность сегодня активно конкурирует с частным бизнесом в борьбе за квалифицированные кадры. Наша задача – создать максимально привлекательные условия труда для сотрудников редких и приоритетных специальностей: инженеров, конструкторов, ИТ-специалистов, операторов станков, квалифицированных рабочих и т.д. Ключевым фактором для привлечения специалистов является решение жилищного вопроса. В рамках пилотного проекта нашим партнером выступило АИЖК, с которым у Корпорации заключено соглашение о сотрудничестве», - отметила руководитель направления финансового планирования и социальных программ Департамента экономики и финансов Госкорпорации Ростех **Юлия Цветкова.**

«Пилотный ЖСК в Истринском районе Московской области будет иметь хорошую транспортную доступность. Участок общей площадью 6,81 Га расположен в непосредственной близости от Волоколамского шоссе, на пересечении с Московским малым кольцом, в 5 километрах от г. Истры и в 33 километрах от МКАД. Местная инфраструктура включает новую школу, 2 детских сада, 2 поликлиники (взрослая и детская), спорткомплекс с бассейном и

图2 诱饵pdf文件

恶意软件分析

Dropper

针对俄罗斯的攻击中释放的可执行文件在主体后隐藏了加密的Bisonal
DLL文件和恶意诱饵文件。一旦执行，dropper就会用RC4和密钥“34123412”解密数据，保存在下面的路径下并执行。

Type	PATH	SHA256
Dropper EXE	N/A	b1da7e1963dc09c325ba3ea2442a54afea02929ec26477a1b120ae44368082f8
Bisonal DLL	C:\Windows\Temp\pvcu.dll	1128D10347DD602ECD3228FAA389ADD11415BF6936E2328101311264547AFA75
Russian Decoy PDF	C:\Windows \Temp\Комплексный проект по созданию жилищно-строительных кооперативов для работников оборонки.pdf	F431E0BED6B4B7FFEF5E40B1B4B7078F2538F2B2DB2869D831DE5D7DF26EE6CD

表 1. 针对俄罗斯的攻击文件哈希和路径
Dropper会创建下面的注册表记录，在计算机重启后执行Bisonal样本：

```
HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Run\"vert" = "rundll32.exe c:\windows\temp\pvcu.dll ,
Qszdez"
```

主模块

DLL
(pvcu.dll)是Bisonal恶意软件，但使用的是不同的C2通信密码。据报道，2014年和2015年Bisona使用的XOR运算来隐藏主体中的C2地址字符串。本样本中的Bisonal使用的

加密类型的变化会导致大量的代码重写，比如网络通信过程、驻留的方法等。比如，2012年的Bisonal样本使用send()和recv()
API与C2服务器通信；而变种使用的是HttpSendRequest()和InternetReadFile()这一类的网络API。

最近攻击中的Bisonal变种用HTTP POST方法在TCP 443端口上与硬编码的C2地址通信。

- kted56erhg.dynssl[.]com
- euiro8966.organiccrap[.]com

上面的域名是由免费的DDNS服务提供的，解析的IP地址为116.193.155[.]38。

当Bisonal变种与C2进行通信时，恶意软件会发送含有静态字符串"ks8d"和"akspbu.txt"、被黑机器IP地址的HTTP POST请求给C2服务器。

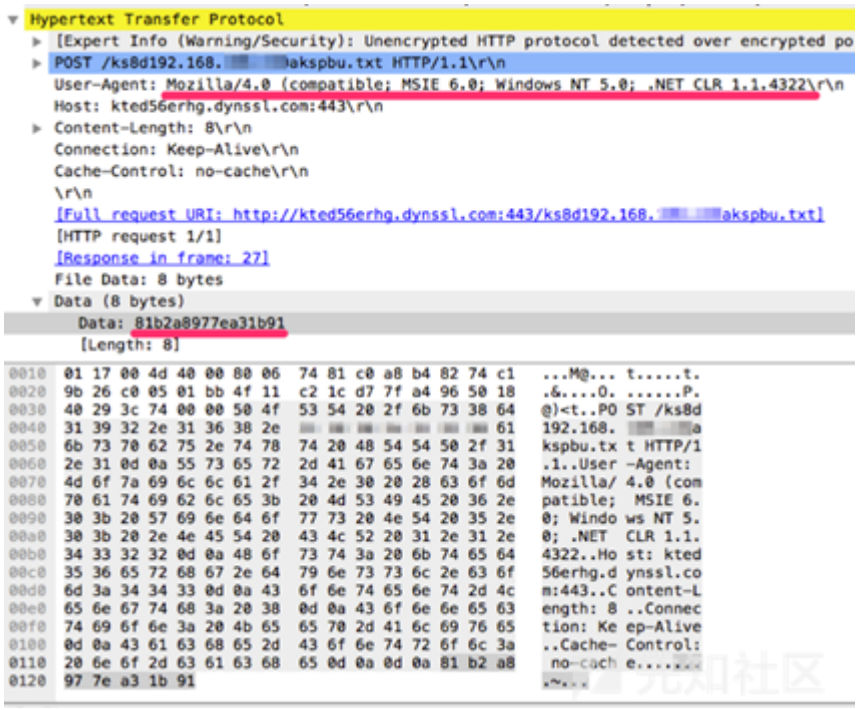


图3. 初始的网络C2

大家可能注意到了User Agent请求头中缺右括号。该字符串是硬编码到恶意软件变种中的，研究人员一共收集了超过230个Bisonal
样本，但只有14个使用这种不完整的User Agent字符串。

目前还不清楚是作者在开发时写漏了还是故意用该字符串来验证到C2的连接。但研究人员认为这可以作为Bisonal感染的网络日志IoC。

C2通信

被感染的另一个标志是初始连接过程中发送给C2的数据。Bisonal变种在与C2通信时间，会在前8个字节中发送唯一的id号和后门命令。恶意软件在初始连接时会发送硬编码

对静态值加密后，后门会发送相同的数据前8字节（81b2a8977ea31b91）给C2。然后接受来自受害者机器的初始信标，C2会返回一个session
id号和后门命令。session id号就是与C2通信的流量一致的。然后恶意软件会在受害者系统上处理给定的命令，并将含有session
id号和后门命令号的结果返回给C2。然后C2会响应相同的session id号。之后，后门会等待5秒钟然后用相同的session id号与C2重新通信。

下图是对命令get system info的响应示例。C2与Bisonal样本的真实流量为左图，解密的payload为右图。第一个DWORD（4字节）是给定的session
id（0x00000003），下一个DWORD是后门命令0x000000C8。解密的payload中的偏移8处，是攻击活动或目标代码（代号），本例中是0425god。

图4 解密后的payload

下图是Bisonal和C2的会话session：

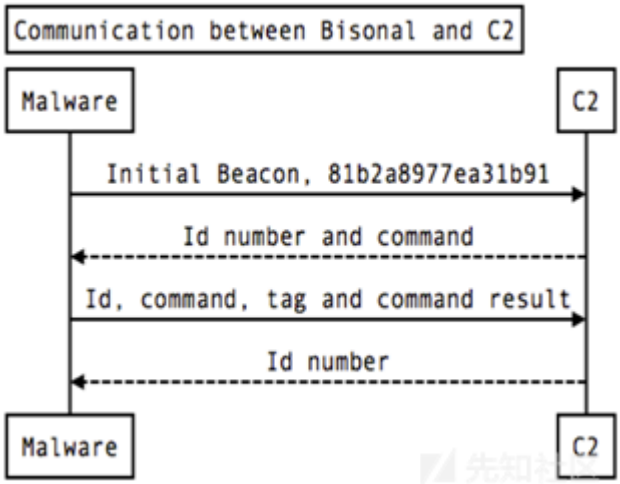


图5. Bisonal C2通信流

下表是恶意软件样本支持的后门命令：

Command	Meaning
0x000000C8	gets system info
0x000000C9	gets running process list
0x000000CA	terminates process
0x000000CB	accesses cmd shell
0x000000CD	downloads file
0x000000CF	executes file
0x000000D1	creates file

表2 后门命令

西里尔(Cyrillic)字母

Bisonal
恶意软件攻击的区域主要是日本、韩国和俄罗斯。研究人员发现针对俄罗斯企业进行攻击的样本中还有一个特点就是会进行Cyrillic语言检查。当后门接收到shell access命令后，就会检查被黑系统的代码页面。如果语言是Cyrillic，而且命令不是ipconfig，就将命令结果文本从Cyrillic变为UTF-16编码。其他模式Windows ANSI代码的页面也会转变为UTF-16编码。

恶意软件作者只针对Cyrillic转变为UTF-16的原因并不明确。Windows
ANSI代码页支持ASCII码字符和非ASCII码字符，UTF-16最多支持Unicode编码的100万字符。为了避免破坏结果中的Cyrillic字符，开发者将这段代码加入到恶意软件中了。

```
.text:10002071                 cmp     [esp+0A90h+codepage], 866 ; Cyrillic
.text:10002079                 jnz     short cp_is_not_Cyrillic
.text:1000207B                 push    offset aIpconfig ; "ipconfig"
.text:10002080                 push    offset shell_command ; wchar_t *
.text:10002085                 call    _wcscmp
.text:1000208A                 mov     ecx, [esp+0A98h+NumberOfBytesRead]
.text:1000208E                 add     esp, 8
.text:10002091                 lea     edx, [esp+0A90h+WideCharStr]
.text:10002098                 test    eax, eax
.text:1000209A                 push    ecx
.text:1000209B                 push    edx
.text:1000209C                 lea     eax, [esp+0A98h+Buffer]
.text:100020A3                 push    0FFFFFFFFh
.text:100020A5                 push    eax
.text:100020A6                 push    ebx
.text:100020A7                 jz      short command_is_ipconfig
.text:100020A9                 push    866
.text:100020AE                 jmp     short command_is_not_ipconfig
.text:100020B0 ; ---------------------------------------------------------------
.text:100020B0
.text:100020B0 cp_is_not_Cyrillic:                     ;
.text:100020B0                 mov     ecx, [esp+0A90h+NumberOfBytesRead]
.text:100020B4                 lea     edx, [esp+0A90h+WideCharStr]
.text:100020BB                 push    ecx             ; cchWideChar
.text:100020BC                 push    edx             ; lpWideCharStr
.text:100020BD                 lea     eax, [esp+0A98h+Buffer]
.text:100020C4                 push    0FFFFFFFFh      ; cbMultiByte
.text:100020C6                 push    eax             ; lpMultiByteStr
.text:100020C7                 push    ebx             ; dwFlags
.text:100020C8
.text:100020C8 command_is_ipconfig:                    ;
.text:100020C8                 push    ebx             ; CodePage
.text:100020C9
.text:100020C9 command_is_not_ipconfig:                ;
.text:100020C9                 call    ebp ; MultiByteToWideChar
```

图6. 检查Cyrillic字符集

shell access后门命令中的
Cyrillic/ipconfig检查存在于一些早期的Bisonal样本中。样本43459f5117bee7b49f2cee7ce934471e01fb2aa2856f230943460e14e19183a6中就含有maker字符串

```
.data:71004010 aBisonal        db 'bisonal',0
.data:71004018 aUzqqvyzm1spptv db 'uzqqvyzm&&',27h,'1spptvq1~k',0
.data:71004018                                         ; DATA XREF: StartAddress+68↑o
.data:71004018                                         ; StartAddress:loc_71002384↑r ...
```

图7. ‘bisonal’ marker字符串

针对韩国的攻击活动

与攻击俄罗斯企业的Bisonal变种类似，针对韩国企业攻击的Bisonal变种也伪装成pdf文档。

图8. 恶意软件伪装成pdf文档

Dropper可执行文件会安装Bisonal和一个诱饵文件到表3中的路径中。

Type	PATH	SHA256
Dropper EXE	N/A	0641fe04713fbdad272a6f8e9b44631b7554dfd1e1332a8afa767d845a90b3fa
Bisonal EXE	%Temp%\[random].tmp	359835C4A9DBE2D95E483464659744409E877CB6F5D791DAA33FD601A01376FC
Korean Decoy PDF	[dropper path]\[same file name without .exe].pdf	B2B764597D097FCB93C5B11CBD864AB1BCB894A2A1E2D2DE1C469880F612431C

表 3 针对韩国的攻击中的文件哈希和系统安装路径

虽然针对韩国和俄罗斯攻击的两个dropper样本的功能看着非常相似，实际上样本的dropper代码是完全不同的。

针对韩国攻击的dropper会安装Bisonal
EXE文件和诱饵pdf文件。这些文件都是不加密的，dropper中exe和pdf文件的偏移量加在了dropper文件的结尾。针对俄罗斯攻击的样本中，这些文件的偏移量是硬编码在

诱饵文件的文件名也与dropper文件的文件名有关。Dropper代码会在相同目录下创建一个pdf文件，文件名与诱饵文件名相同，并将扩展名从exe变为pdf。比如，如果文件

Dropper会在%Temp%目录下创建2个随机4位数字名的VBS脚本，其中一个脚本会打开诱饵pdf文件，另一个删除dropper和VBS脚本。

诱饵pdf文件的内容是韩国海岸警卫队的工作描述，与韩国海岸警卫队官网上的内容一致。根据pdf文件的元数据，研究人员认为攻击者将官网的附件直接转为pdf文件了。

图8. 诱饵文件的Metadata

主EXE

安装的EXE文件与针对俄罗斯企业的Bisonal变种的DLL版本几乎是相同的。EXE文件与DLL文件有三点不同，分别是：

- 自己创建注册表；
- C2域名；
- 目标和攻击活动代码（代号）。

下面是Bisonal EXE的行为分析。

- 会创建注册表`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"mismyou" = %Temp%[random].tmp`来达到驻留的目的。因为DLL的dropper会创建注册表，所以DLL版本不会创建注册表。
- 使用RC4加密算法和key 78563412解密C2域名地址。
- 用含有不完整User Agent字符串（`Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322`）的 HTTP POST方法连接`hxxp://games.my-homeip[.]com:443/ks8d[ip address]akspbu.txt`。
- 发送同样的初始信标值`81b2a8977ea31b91`到C2服务器。
- 使用不同的目标或活动代码"pmo"。

- 有相同的后门命令，以0x000000C8开头。
- 也检查代码页和shell access中的命令，并将文本从Cyrillic转化为UTF-16编码。

Year	Target Country	Campaign or Target Code	SHA256	Cipher	Bisonal Marker	Cyrillic/ ipconfig check	C2
2012	unidentified	1031	43459f5117bee7b49f2cee7ce934471e01fb2aa2856f230943460e14e19183a6	XOR	YES	YES	jennifer998.lookin[.]at, 196.44.49[.]154
2014	South Korea	0919-1	dfa1ad6083aa06b82edfa672925bb78c16d4e8cb2510cbe18ea1cf598e7f2722	RC4	NO	YES	www.hosting.tempors.com
2018	Russia	0425god	1128D10347DD602ECD3228FAA389ADD11415BF6936E2328101311264547AFA75	RC4	NO	YES	kted56erhg.dynssl[.]com, euiro8966.organiccrap[.]com
2018	South Korea	pmo	359835C4A9DBE2D95E483464659744409E877CB6F5D791DAA33FD601A01376FC	RC4	NO	YES	games.my-homeip[.]com

表 4 Bisonal样本总结

攻击活动总结

虽然Bisonal恶意软件已经活跃7年了，而且每隔一段时间就会更新一次，攻击者一直使用同样的高级配置。攻击的特点包括：

- 攻击目标为与韩国、俄罗斯、日本的政府、军事和国防行业相关的企业和组织；
- 使用动态DNS作为C2服务器；
- 使用目标和攻击活动的代码与C2通信来记录受害者或攻击活动的链接；
- 将恶意软件伪装成PDF、office文档或Excel文件；
- 使用诱饵文件和恶意PE文件；
- 在一些实例中，含有处理俄语操作系统上的西里尔(Cyril)字符的代码。

针对俄罗斯和韩国的攻击活动中都有上述特征。