登录

“MartyMcFly”调查：追踪anchors-chain

A1oha / 2018-11-23 09:00:00 / 浏览数 2615 技术文章 技术文章 顶(0) 踩(0)

背景

10月17日，我们披露了“MartyMcFly”威胁活动Rif. Analysis，这群未知的攻击者的将意大利海军作为目标。该分析报告被卡巴斯基ICS CERT引用，并进一步说明：该组织在德国、西班牙、印度等多个国家均存在威胁活动。由于卡巴斯基的扩展分析，我们决定收集更多威胁指标，为此我们与Fincantieri公司

恶意邮件

Fincantieri安全团队给我们共享了一份恶意电子邮件副本，
这份邮件是Yoroi的网络安全防御中心在10月9日至15日之间截获的。由于SMTP头部中发件人与域数据不一致，邮件显得可疑：

```
From: alice.wu@anchors-chain.com

Subject: Quotation on Marine Engine & TC Complete

User-Agent: Horde Application Framework 5

X-PPP-Vhost: jakconstruct.com
```

电子邮件从“ jakconstruct.com”域名相关的邮箱发送，该域名归quatari的AK建筑公司所有，这表明他们的电子邮件系统可能遭到了滥用。

```
X-PPP-Message-ID: <20180820010543.32473.21538@w3i.email>
X-PPP-Vhost: jakconstruct.com

jakconstruct.com.       3599    IN      MX      10 mxb.w3i.email.

Authentication-Results: w3i.email;
        spf=pass (sender IP is 127.0.0.1) smtp.mailfrom=alice.wu@anchors-chain.com smtp.helo=w3i.email
```

图-1 SMTP头中的smtp详细信息

在SMTP头中，from字段里的“anchors-chain.com”域名早在恶意邮件被发送前几周就已被购买，域名拥有者于2018年6月21日在“NameSilo，LLC”进行了注册，并设置了隐

```
Domain Name: anchors-chain.com
Registry Domain ID: 2277474287_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2018-06-21T07:00:00Z
Creation Date: 2018-06-20T07:00:00Z
Registrar Registration Expiration Date: 2019-06-20T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Reseller: QHOSTER.COM
Domain Status: clientTransferProhibited https://www.icann.org
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
```

图-2 “anchors-chain.com”的Whois数据

从2018年6月22日到9月2日，该域名解析为188.241.39.10，为Fast Serv
Inc.所有。域名在托管时，有时会被非法使用（例如：被当做C2服务器，下发恶意软件，窃取个人信息）然而，在撰写本文时，该域名已经下线，所以难以确定在“
MartyMcFly ”活动中，它是否被用作跳转链接。

此外，“ anchor s -chain.com “域名提到了一家亚洲公司，该公司以生产锚链为主，在造船业有广泛的客户，那就是“Asian Star Anchor Chain Co.
Ltd.”（亚星星锚链有限公司），二者域名几乎相同，字母“ s
”是攻击者注册的域名与合法域名之间的唯一区别。此外，邮件主体使用的中文，在签名处有只指向公司另一个合法域名的链接，可以确定攻击者想要冒充ASAC的工作人员发

图-3 恶意电子邮件

附件

该电子邮件消息中包含名为“Marine_Engine_Spare__Parts_Order.pdf”的pdf文档，该文档最初使用“ Microsoft Word 2013 ”撰写，然后在“ Online2PDF.com ”在线转换为PDF格式。

此文档不包含任何javascript脚本或漏洞利用代码，但文档页面中的链接试图引诱受害者在所谓的“ Adobe 在线保护”下打开pdf文档。这个嵌入式链接指向短域名“ Ow.ly ”中的外部资源。

图-4 恶意pdf文档

所指向的外部链接“ http://ow.ly/laqJ30lt4Ou ”
因“垃圾邮件”问题已被停用，在撰写本文时已无法访问。然而，通过分析可按时间段回溯攻击事件的沙盒生成的报告，可以部分地重现payload执行后的状态。

图-5 附件的进程树

动态跟踪拓扑中记录了“ .usa.cc ”TLD 上两个可疑域名的网络行为，它们是在“ iexplore.exe ”浏览器进程启动后发起的：分别“ wvpznpgahbtoobu.usa.cc ”和“ xtyenvunqaxqzrm.usa. cc ”。

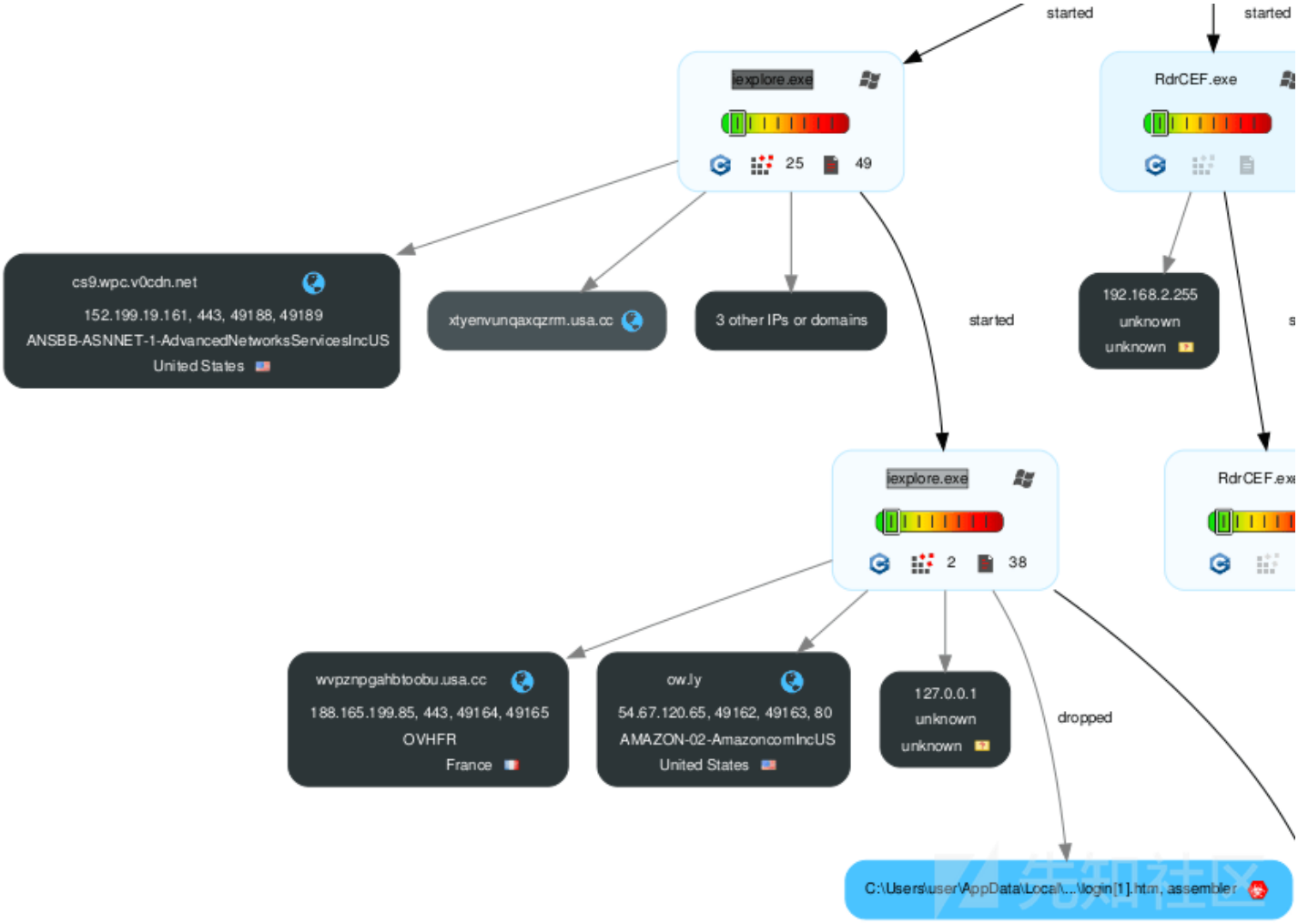

图-6 截获的DNS请求

第一个网络交互与pdf附件" http://ow.ly/laqJ30lt4Ou " 内的嵌入链接相关，将会重定向到该短域名下的另一个资源。

Aug 21, 2018 15:52:09.438220024 CEST	1	IN	HTTP/1.1 301 Moved Permanently Location: http://ow.ly/Kzr430lt4NV?platform=hootsuite Connection: close Content-Length: 0

图-7 重定向到第二个ow.ly url

请求" http://ow.ly/Kzr430lt4NV "，将由一个HTTP 301重定向到与之前标识的" usa.cc "相关的HTTPS资源：

Aug 21, 2018 15:52:09.638497114 CEST	2	IN	HTTP/1.1 301 Moved Permanently Location: https://wvpznpgahbtoobu.usa.cc/wvpznpgahbtoobu/usaadobe/lexorder.php?platform=hootsuite Connection: close Content-Length: 0

图-8 重定向到"wvpznpgahbtoobu.usa.cc"

通过分析会话期间截获的SSL / TLS流量，显示它与ip地址188.165.199.85有多次连接，这是一台由OVH SAS托管的专用服务器。其SSL证书由"cPanel，Inc"CA发布，自2018年8月16日生效.由于在Subject字段中找到了通用名称" CN = wvpznpgahbtoobu.usa.cc "，因此该加密证书可能与先前讨论的HTTP 301重定向有关。

Subject	Issuer	Not Before	Not After
CN=wvpznpgahbtoobu.usa.cc	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	Thu Aug 16 02:00:00 CEST 2018	Thu Nov 15 00:59:59 CET 2018

图-9 "wvpznpgahbtoobu.usa.cc"SSL证书详细信息

另一个SSL / TLS链接也是与“xtyenvunqaxqzrm.usa.cc ”相关的流量，指向的 ip地址同样为188.165.199.85

Aug 21, 2018 15:52:15.830455065	443	49168	188.165.199.85	192.168.2.2	CN=xtyenvunqaxqzrm.usa.cc	CN="cPanel, Inc. Certification	Fri Aug 17	Fri Nov 16

图-10 “xtyenvunqaxqzrm.usa.cc”SSL证书详细信息

OSINT调查整理了过去“ xtyenvunqaxqzrm.usa.cc ”被恶意利用的证据，例如，2018年8月23日urlquery发布的报告显示，曾经可以通过访问“ https：// xtyenvunqaxqzrm .usa.cc / maeskl ” 跳转到一个钓鱼网站 i nes / Maerskline / maer.php “，这是一个冒充“ 马士基
“控股航运公司门户网站的登录页面，该公司是一家跨国物流公司，同时也是世界上最大的集装箱运输公司之一。

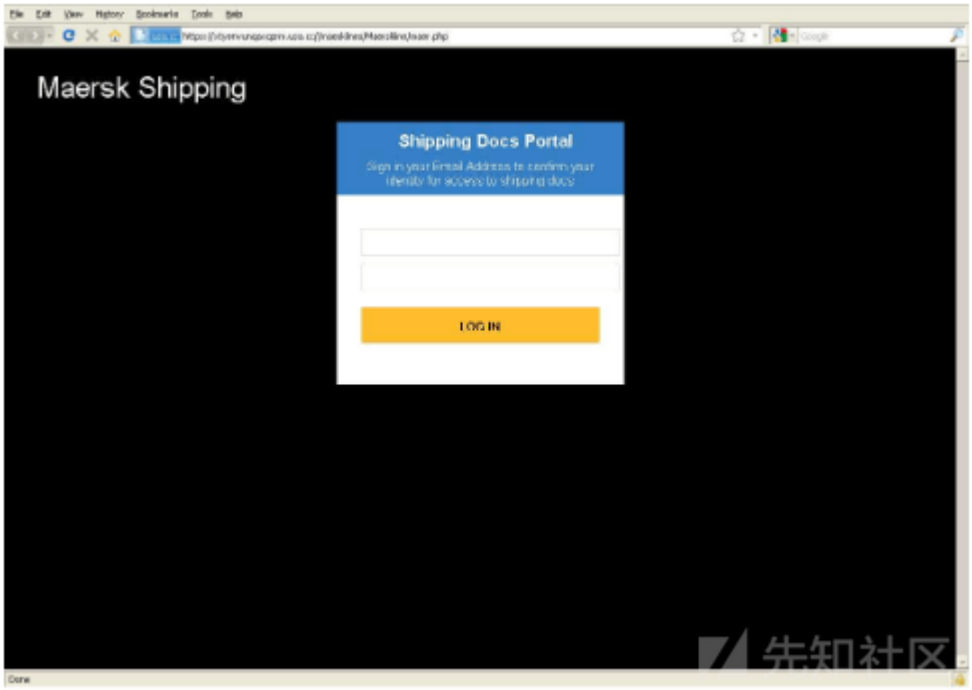

图-11 托管在xtyenvunqaxqzrm.usa.cc上的钓鱼页面

在动态执行表中的元素表明了“ xtyenvunqaxqzrm.usa.cc ”的OSINT信息与附件本身之间的兼容性：在沙盒的自动分析部分，可以看到“ login.html
”在执行完成后被删除，该文件已被VirusTotal归类为网络钓鱼模板（ hash 4cd270fd943448d595bfd6b0b638ad10 ）。

Antivirus Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Marine Engine Spare Parts Order_first.pdf	12%	virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DEWWYACU\login[1].htm	100%	Avira	HTML/Infected.Page.Gen	

图-12 login.html页面在执行期间被删除

结论

在与Fincantieri安全团队的联合分析中收集的证据表明，一些未查明的威胁活动企图入侵意大利海军部门。至此为止我们无法确认两次有计划的攻击是否均为“MartyMcFly”

- 冒充海军部队服务提供商及卫星公司.
- 精心选择与知名公司合法域名类似的域名
- 构造包含外部链接、文档 等内容的邮件，与真实邮件保持格式一致.
- 可能使用 “Microsoft Word 2013”

最后，感谢Fincantieri安全团队的同事分享这些攻击数据，帮助我们调查此次威胁事件。

IOC

下面是分析过程中总结的一些ioc:

垃圾邮件：

- anchors-chain.com
- 188.241.39.10
- alice.wu@anchors-chain.com
- Quotation on Marine Engine & TC Complete
- jakconstruct.com

url:

- http://ow.ly/laqJ30lt4Ou
- http://ow.ly/Kzr430lt4NV
- wvpznpgahbtoobu.usa.cc
- xtyenvunqaxqzrm.usa.cc
- https://wvpznpgahbtoobu.usa.cc/wvpznpgahbtoobu/usaadobe/lexorder.php
- 188.165.199.85

Hash:

- 7c9576123a35749c1699f53a1206577e
- 4cd270fd943448d595bfd6b0b638ad10

上一篇：如何在受限环境中利用Firefox... 下一篇：[红日安全]代码审计Day17 -...

1. 0 条回复
   - 动动手指，沙发就是你的了！