2017 年 10 月 24 日，星期二

威胁聚焦：追踪 BadRabbit 勒索软件

注：本文旨在介绍 Talos 对一项新威胁进行的自发研究。这类信息只能视为初步信息，并将随着研究继续持续更新。

2017 年 10 月 24 日，思科 Talos 接到警报，网络上出现了一种大规模的勒索软件攻击活动影响到了东欧和俄罗斯的很多组织。与以前一样，我们迅速行动起来，评估局势并确保保护客户不受此勒索软件和其他新出现的威胁影响。

最近几个月来已经出现了好几次大规模的勒索软件攻击活动。这次的勒索软件与 Nyetya 存在一些相似之处，也是以 Petya 勒索软件为基础，但是对大部分代码进行了改写。这次传播的病毒似乎没有我们最近发现的供应链攻击那么复杂。

传播

Talos 进行了评估，确信攻击者通过“路过式下载”方法传播了一种虚假 Flash Player 更新并通过此更新入侵系统。攻击者将被入侵的网站重定向至 BadRabbit，受影响的网站很多，主要位于俄罗斯、保加利亚和土耳其。

当用户访问被入侵的网站时，系统会重定向至 1dnscontrol[.]com 这一托管该恶意文件的网站在下载实际的恶意文件之前，攻击者会向静态 IP 地址 (185.149.120[.]3) 发送一个 POST 请

求。我们发现该请求发布到了“/scholasgoogle”静态路径，并向用户提供代理、引用站点、Cookie 和域名。在发布 POST 请求之后，系统从 1dnscontrol[.]com 的两个不同路径 /index.php 和 /flash_install.php 下载了植入程序。尽管使用了两个路径，但却只下载了一个文件。根据当前信息，在服务器 1dnscontrol[.]com 被入侵之前，该恶意软件似乎已经活动了大约六小时。我们观察到的首次下载时间大约在 UTC 时间 2017 年 10 月 24 日早上 8:22。

植入程序 (630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da) 需要用户协助实施感染，而未使用任何漏洞攻击包来直接入侵系统。该植入程序包含 BadRabbit 勒索软件。该植入程序安装之后，它会使用一个 SMB 组件来进行内部扩散和进一步感染。其做法似乎是组合使用随附的弱凭证列表和与 Nyetya 所用的类似的 mimikatz 版本下面是我们观察到的用户名/密码组合的列表。请注意，这与 1995 年臭名昭著的“黑客”存在重合。

.rdata:1001...	00000008	C (1...	god
.rdata:1001...	00000008	C (1...	sex
.rdata:1001...	0000000E	C (1...	secret
.rdata:1001...	0000000A	C (1...	love
.rdata:1001...	00000008	C (1...	321
.rdata:1001...	0000000E	C (1...	123321
.rdata:1001...	0000000A	C (1...	uiop
.rdata:1001...	0000000A	C (1...	zxcv
.rdata:1001...	0000000E	C (1...	zxc321
.rdata:1001...	0000000E	C (1...	zxc123
.rdata:1001...	00000008	C (1...	zxc
.rdata:1001...	00000014	C (1...	qwerty123
.rdata:1001...	0000000E	C (1...	qwerty
.rdata:1001...	0000000C	C (1...	qwert
.rdata:1001...	0000000A	C (1...	qwer
.rdata:1001...	0000000E	C (1...	qwe321
.rdata:1001...	0000000E	C (1...	qwe123
.rdata:1001...	00000008	C (1...	qwe
.rdata:1001...	00000008	C (1...	777
.rdata:1001...	0000000C	C (1...	77777
.rdata:1001...	0000000C	C (1...	55555
.rdata:1001...	0000000E	C (1...	111111
.rdata:1001...	00000012	C (1...	password
.rdata:1001...	00000010	C (1...	test123
.rdata:1001...	00000020	C (1...	admin123Test123
.rdata:1001...	00000012	C (1...	Admin123
.rdata:1001...	00000010	C (1...	user123
.rdata:1001...	00000010	C (1...	User123
.rdata:1001...	00000012	C (1...	guest123
.rdata:1001...	00000012	C (1...	Guest123
.rdata:1001...	00000022	C (1...	administrator123
.rdata:1001...	00000022	C (1...	Administrator123
.rdata:1001...	00000016	C (1...	1234567890
.rdata:1001...	00000014	C (1...	123456789
.rdata:1001...	00000012	C (1...	12345678
.rdata:1001...	00000010	C (1...	1234567
.rdata:1001...	0000000E	C (1...	123456
.rdata:1001...	0000000C	C (1...	12345
.rdata:1001...	0000000A	C (1...	1234
.rdata:1001...	00000008	C (1...	123
.rdata:1001...	0000000A	C (1...	test
.rdata:1001...	00000014	C (1...	adminTest
.rdata:1001...	0000000A	C (1...	user
.rdata:1001...	0000000C	C (1...	guest
.rdata:1001...	0000001C	C (1...	administrator
.rdata:1001...	0000000A	C (1...	alex
.rdata:1001...	00000012	C (1...	netguest
.rdata:1001...	00000014	C (1...	superuser
.rdata:1001...	00000012	C (1...	nasadmin
.rdata:1001...	00000010	C (1...	nasuser
.rdata:1001...	00000008	C (1...	nas
.rdata:1001...	00000012	C (1...	ftpadmin
.rdata:1001...	00000010	C (1...	ftpuser
.rdata:1001...	0000000A	C (1...	asus
.rdata:1001...	0000000E	C (1...	backup
.rdata:1001...	00000012	C (1...	operator

我们观察到的密码列表

尽管已经制作初步报告，但是我们目前没有任何证据表明攻击者利用了 EternalBlue 漏洞攻击包来传播感染。然而，我们的研究还在继续，如果获得更多信息，我们将及时公布。

技术详情

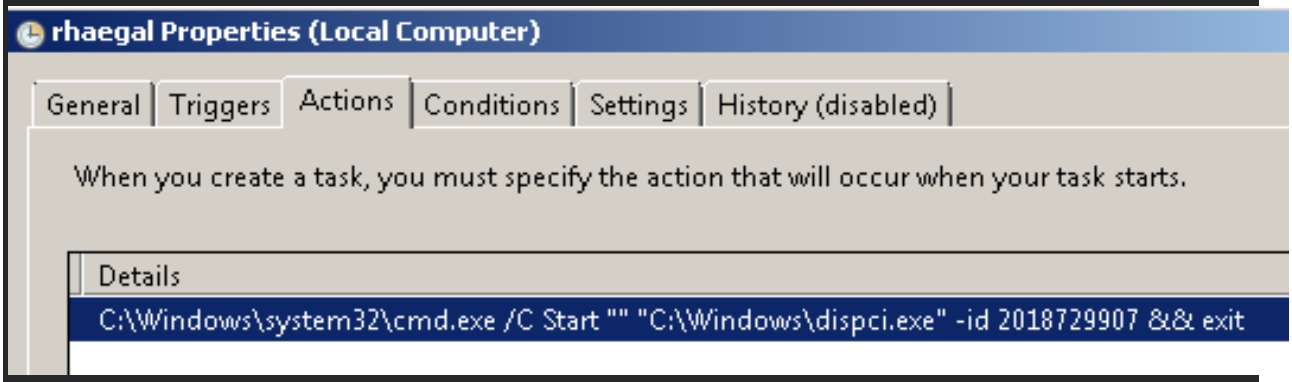
该恶意软件包含一个负责提取和执行蠕虫负载的植入程序。这个负载包含以下存储于资源中的附加二进制文件（使用 zlib 压缩）：

- 若干与 DiskCryptor 关联的合法二进制文件（2 个驱动程序 x86/x64 和 1 个客户端）
- 2 个类似于 mimikatz 的二进制文件 (x86/x64)，与 Nyetya 中发现的样本相似。这是一种常见的开源工具，用于通过几种不同的方法从计算机内存中恢复用户凭证。

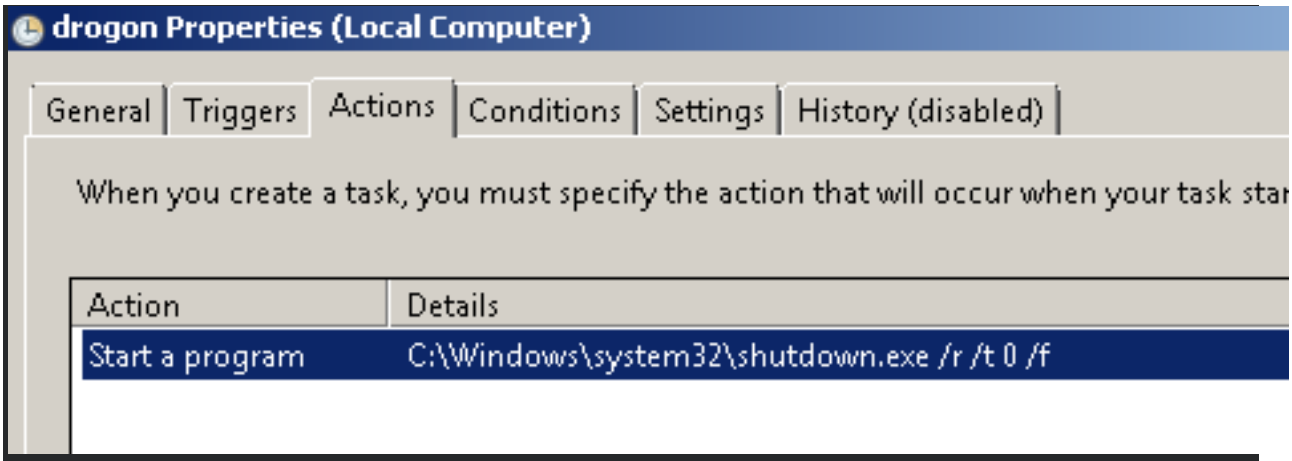
该植入程序向 C:\Windows\ 目录植入若干文件。攻击者利用 Nyetya 攻击活动中相同的方法执行那些类似于 mimikatz 的二进制文件。负载和凭证窃取程序之间使用指定管道命令进行通信，下面是一个这种管道命令的示例：

```
C:\WINDOWS\561D.tmp \\.\pipe\{C1F0BF2D-8C17-4550-AF5A-65A22C61739C}
```

然后，该恶意软件使用 RunDLL32.exe 执行恶意软件并继续进行恶意操作。随后，该恶意软件使用如下屏幕截图所示的参数创建一个预定任务：

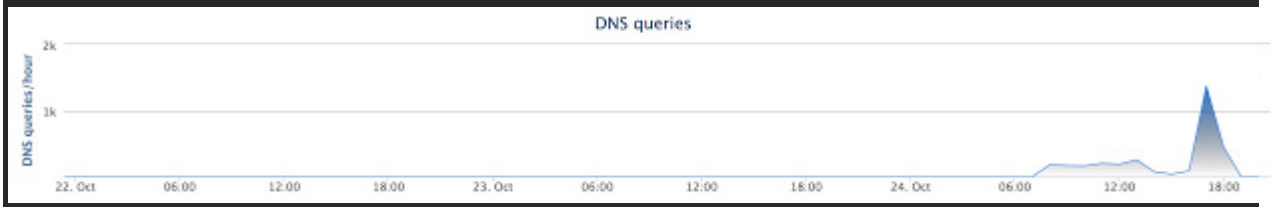


除了上述预定任务，该恶意软件还会再创建一个负责重启系统的预定任务。这第二个任务不会立即执行，而是按照计划稍后执行。



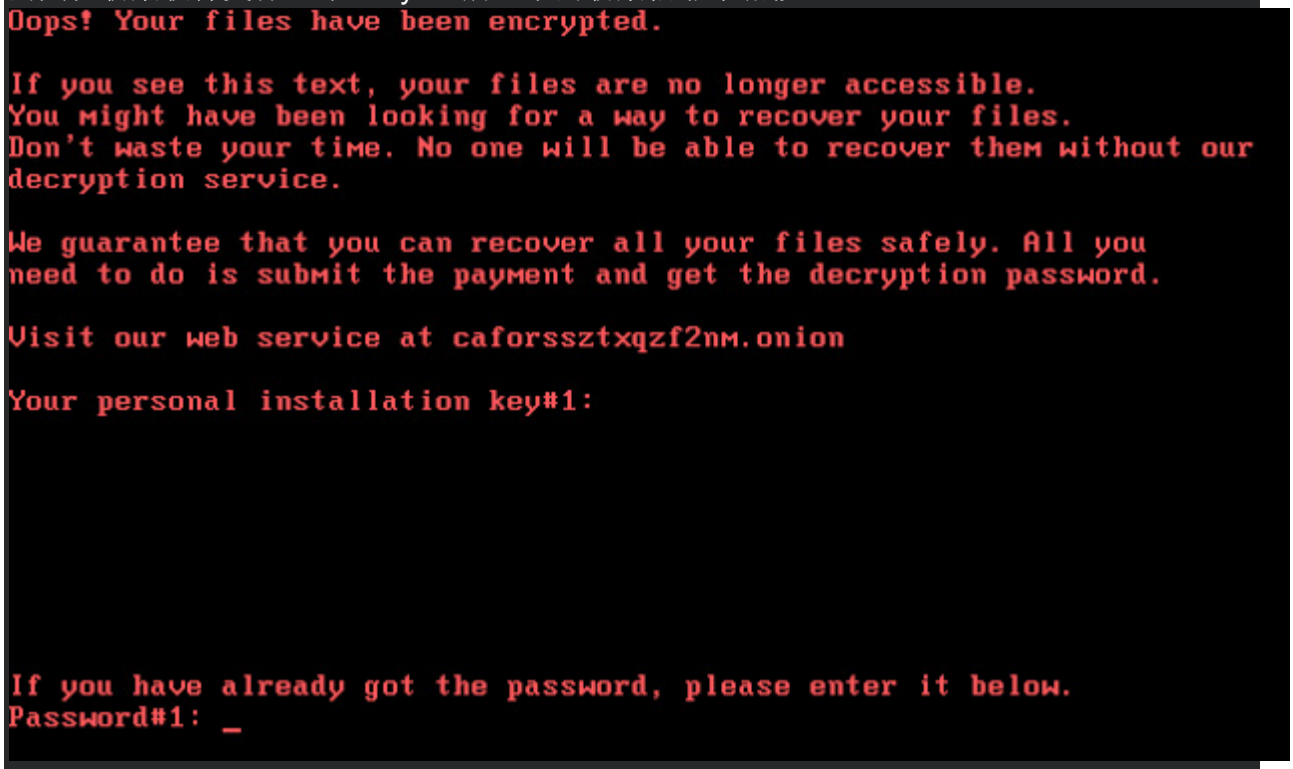
如果感觉这些预定任务的名称看起来很熟悉，那是因为它们引用了《权利的游戏》的内容，具体而言它们与里面那些龙的名字是一致的。该恶意软件还在受感染用户的桌面上创建了一个名为 DECRYPT 的文件。如果受害者执行此文件，系统会显示一封如下所示的勒索信。

为了揭示这类威胁在全球的传播速度有多快，我们绘制了下图，从中可以看出，在用于传播那个在受害者系统上植入恶意软件的虚假 Adobe Flash 更新的域中，其中一个域就存在非常活跃的 DNS 相关活动。

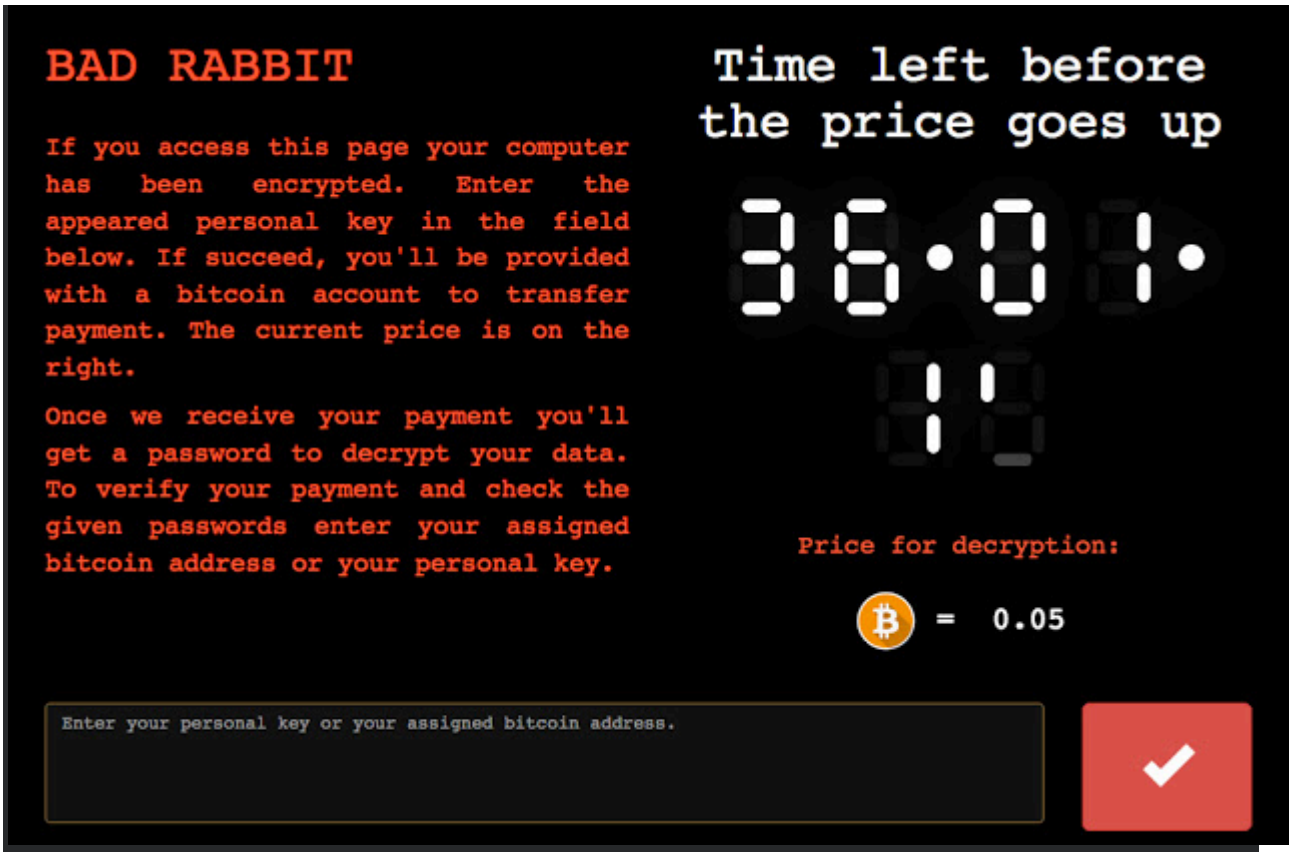


该恶意软件修改了被感染系统硬盘的主启动记录 (MBR)，将启动过程重定向到恶意软件制作

者代码中，从而显示勒索信。系统重启之后显示的勒索信如下，与今年其他重大攻击中发现的其他勒索软件变体（即 Petya）所显示的勒索信非常相似。



以下是 TOR 网站显示的付款页面：



结论

这次攻击活动又一次证明了，勒索软件可以如何高效地使用 SMB 等辅助传播方法进行快速传播。在此例中，初始攻击媒介不是复杂的供应链攻击，而是利用被入侵的网站实现的“路过式下载”基本攻击。这正在迅速成为威胁形势的新常态。威胁传播速度越快，留给防御者的响应时间就越短，势必造成巨大的危害。无论攻击者是想谋取钱财，还是想蓄意破坏，勒索软件都是首选威胁方式。只要还有牟利或造成破坏的可能，这类威胁就会继续肆虐。

这类威胁也扩大了需要处理的另一重要问题，那就是对用户进行宣传教育。在此次攻击中，用户需要协助攻击者实现初步感染。如果用户不安装那个 Flash 更新，就不会帮助完成这个攻击过程，该恶意软件就会保持良性状态，不会对该地区造成严重破坏。一旦用户帮助完成了初步感染，该恶意软件就可以利用现有的方法（例如 SMB）在整个网络内传播病毒，而无需用户交互。

防护

产品	保护
AMP	✔
CloudLock	不适用
CWS	✔
邮件安全	不适用
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

CWS 或 WSA 的 Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

网络安全设备（例如 NGFW、NGIPS 和 Meraki MX）可以检测与此威胁相关的恶意活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella，我们的安全互联网网关 (SIG)，可阻止用户连接恶意域、IP 和 URL（无论用户是否位于公司网络上）。

此次没有发现攻击者以邮件作为攻击媒介。如果该恶意软件在您网络的这些系统之间传输，将会受到阻止。

感染指标

哈希值 (SHA256)

植入程序：

- 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da

负载：

- 8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93 C:\Windows\dispci.exe (diskcryptor client)
- 682ADCB55FE4649F7B22505A54A9DBC454B4090FC2BB84AF7DB5B0908F3B7806 C:\Windows\cscc.dat (x32 diskcryptor drv)
- 0b2f863f4119dc88a22cc97c0a136c88a0127cb026751303b045f7322a8972f6 C:\Windows\cscc.dat (x64 diskcryptor drv)
- 579FD8A0385482FB4C789561A30B09F25671E86422F40EF5CCA2036B28F99648 C:\Windows\infpub.dat

- 2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035 (mimikatz-like x86)
- 301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcfe347c (mimikat-like x64)

预订任务名称

- viserion_
- rhaegal
- drogon

域

分发域：

- 1dnscontrol[.]com

分发路径：

- /flash_install.php
- /index.php

中间服务器：

- 185.149.120[.]3

引用网站：

- Argumentiru[.]com
- Fontanka[.]ru
- Adblibri[.]ro
- Spbvoditel[.]ru
- Grupovo[.]bg
- www.sinematurk[.]com

隐藏的服务：

- caforssztxqzf2nm[.]onion

发布者：NICK BIASINI；发布时间：16:51
标签：勒索软件、TALOS、威胁研究