BadRabbit 勒索软件攻击事件通告

文档信息

编号	360TI-SE-2017-0012
关键字	BadRabbit Ransomware 勒索软件
发布日期	2017 年 10 月 25 日
更新日期	2017 年 10 月 27 日
TLP	WHITE
分析团队	360 威胁情报中心、360 安全监测与响应中心

通告背景

2017 年 10 月 24 日，一款被命名为“坏兔子”(BadRabbit)的勒索软件被发现大量传播，360 威胁情报中心分析对其进行了技术分析和影响面评估，提供处置建议。

事件概要

攻击目标	特定俄语系网站及相关的访问者
攻击目的	表现为文件加密勒索，不排除实质为破坏性攻击
主要风险	数据损毁，信息丢失
攻击入口	攻击者入侵合法网站分发伪装 Flash 软件的勒索恶意代码，准定向攻击
使用漏洞	无
通信控制	连接 Tor 网络传递密钥，收取赎金
抗检测能力	中
受影响应用	Windows 操作系统
已知影响	目前评估国内受影响用户数量极少，感染用户主要集中在俄罗斯、乌克兰及东欧地区
分析摘要： • 战术	1. 入侵俄语系新闻网站植入恶意代码诱导访问者下载执行看起来是 Flash 升级的勒索软件，执行典型的水坑攻击，投放有一定的定向

• 技术 • 过程	性。 2. 恶意代码执行以后会扫描本地网络的 SMB 共享尝试用一个内置的弱口令列表进行暴破，并使用 NSA 永恒浪漫 SMB 服务漏洞进行攻击，感染更多内网系统。 3. 恶意代码会释放本地认证凭据提取工具 Mimikatz 程序，通过账号信息进行横向移动。 4. 恶意代码复用了 Petya 勒索软件的部分代码，与此家族具有一定的继承性。

事件描述

2017 年 10 月 24 日，一款被命名为“坏兔子”(BadRabbit)的勒索软件在境外发生了一定规模的感染，目前涉及的国家主要有俄罗斯、乌克兰、保加利亚、土耳其和德国，有用户通过水坑攻击被恶意代码加密系统文件要求支付赎金。作为恶意软件分发渠道而被入侵的网站包括俄罗斯的国际文传电讯社、乌克兰基辅的地铁系统、乌克兰敖德萨的国际机场以及乌克兰的基础设施部等多家大型机构。

事件时间线

2017 年 10 月 24 日俄罗斯、乌克兰及东欧地区发现一定规模的勒索软件攻击，大量用户的系统文件被加密要求支付赎金。

2017 年 10 月 25 日主要的防病毒厂商发现此攻击并作出响应。

影响面和危害分析

受恶意代码感染的用户电脑上的文件会被加密并要求支付赎金，超过一定期限赎金会上涨。

根据 360 网络研究院和威胁情报中心的数据评估，此勒索软件目前在国内几乎还没有批量的感染发生，但是需要引起必要的重视并采取应对措施以避免受可能的影响。

处置建议

1. 备份电脑上的重要文件到本机以外的其他机器上，检查组织内部的备份机制是否正常运作。
2. 电脑安装防病毒安全软件，确认规则升级到最新。
3. 检查 SMB 共享是否使用了弱口令，本次事件相关的账号和弱口令列表见附件。

技术分析

BadRabbit 通过水坑攻击将恶意代码植入到合法网站，伪装成 Flash 升级更新弹窗，诱骗用户主动下载运行恶意程序。此恶意程序除了加密受害终端的文档外，还会扫描内网 SMB 共享，使用弱口令和 NSA 永恒浪漫漏洞进行攻击传播。此恶意代码还会释放 Mimikatz 类工具，通过获取登录凭证尝试登录和感染内网其他主机。

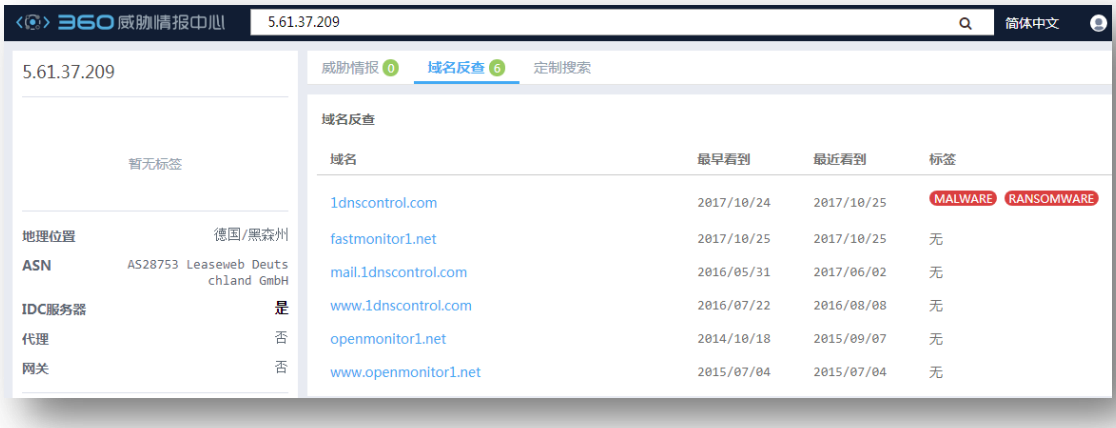
更多技术细节可以参看参考资料的网页。

关联分析及溯源

勒索软件复用了部分 Petya 家族的代码，可以视其与 Petya 家族有一定的继承关系。

勒索软件使用了 1dnscontrol.com 域名作为恶意代码的分发站点，查询 360 威胁情报中心，此域名注册于 2016 年 3 月 22 日并作了隐私保护：

域名解析到 IP 5.61.37.209，此 IP 所绑定其他域名也非常可疑，极有可能为同一攻击团伙所有：



参考资料

https://securelist.com/bad-rabbit-ransomware/82851/

http://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html?m=1

更新历史

时间	内容
2017 年 10 月 25 日	初始报告
2017 年 10 月 27 日	补充利用 NSA 永恒浪漫漏洞的信息

附件

IOC 列表

C&C
caforssztxqzf2nm.onion http://185.149.120.3/scholargoogle/ http://1dnscontrol.com/flash_install.php 1dnscontrol.com
挂马站点
argumentiru.com www.fontanka.ru grupovo.bg www.sinematurk.com www.aica.co.jp spbvoditel.ru argumenti.ru www.mediaport.ua blog.fontanka.ru an-crimea.ru www.t.ks.ua most-dnepr.info osvitaportal.com.ua www.otbrana.com calendar.fontanka.ru

www.grupovo.bg www.pensionhotel.cz www.online812.ru www.imer.ro novayagazeta.spb.ru i24.com.ua bg.pensionhotel.com ankerch-crimea.ru
同源 IP 可疑域名
fastmonitor1.net openmonitor1.net secure-dns1.net

Hash	备注
fbbdc39af1139aebba4da004475e8839	install_flash_player.exe
1d724f95c61f1055f0d02c2154bbccd3	infpub.dat
b14d8faf7f0cbcfad051cefe5f39645f	dispci.exe
b4e6d97dafd9224ed9a547d52c26ce02	cscc.dat
347ac3b6b791054de3e5720a7144a977	Mimikatz x64
37945c44a897aa42a66adcab68f560e0	Mimikatz x86

BadRabbit 尝试暴破的 SMB 用户名和弱口令列表

账号	口令
Administrator	Administrator
Admin	administrator
Guest	Guest
User	guest
User1	User
user-1	user
Test	Admin

root	adminTest
buh	test
boss	root
ftp	123
rdp	1234
rdpuser	12345
rdpadmin	123456
manager	1234567
support	12345678
work	123456789
other user	1234567890
operator	Administrator123
backup	administrator123
asus	Guest123
ftpuser	guest123
ftpadmin	User123
nas	user123
nasuser	Admin123
nasadmin	admin123Test123
superuser	test123
netguest	password
alex	111111
	55555
	77777
	777
	qwe
	qwe123
	qwe321
	qwer
	qwert
	qwerty
	qwerty123

	zxc zxc123 zxc321 zxcv uiop 123321 321 love secret sex god