AhnLab

安全月刊

2021.10 Vol.107

Lockbit 勒索软件

卷土重来的 Lockbit 勒索软件，企业应加强防范

威胁全球企业的勒索软件，不仅攻击次数增长迅猛，而且攻击类型也变得更加多样化。其中，被归类为相对较新的LockBit勒索软件正在成为主要威胁，因为它在出现后的两年内攻击了包括韩国在内的全球主要企业。

在本文中，我们将介绍LockBit勒索软件的特征和受害事例，并分析了具体的攻击方式。

LockBit勒索软件（LockBit Ransomware）最早出现于2019年9月，它采用了勒索软件即服务（Ransomware as a Service: RaaS）的形式，并在过去两年中，攻击了美国、中国、印度、印度尼西亚、乌克兰、英国、法国、德国等欧洲国家的企业及政府组织。

早期的Lockbit勒索软件被称为“ABCD勒索软件”，因为在加密过程中使用扩展名“.abcd”重命名文件，现在该勒索软件使用的扩展名是 “.lockbit”，并于2021年6月更新为2.0版本，目前正在传播中。该版本增加了通过滥用 Active Directory（AD）组策略加密整个Windows域的功能。安全公司趋势科技（Trend Micro）表示，在2021年7月1日至8月15日期间，检测到针对智利、意大利、台湾和英国的企业和组织尝试攻击的行为。此外，自2021年7月13日起停止分发BlueCrab（Sodinokibi，REvil）勒索软件之后，Lockbit勒索软件的传播量进一步增加。

2021年8月，有媒体报道称，韩国公司的两家美国子公司也遭到了袭击，对此我们应该要提高警惕。

LockBit 勒索软件的特点

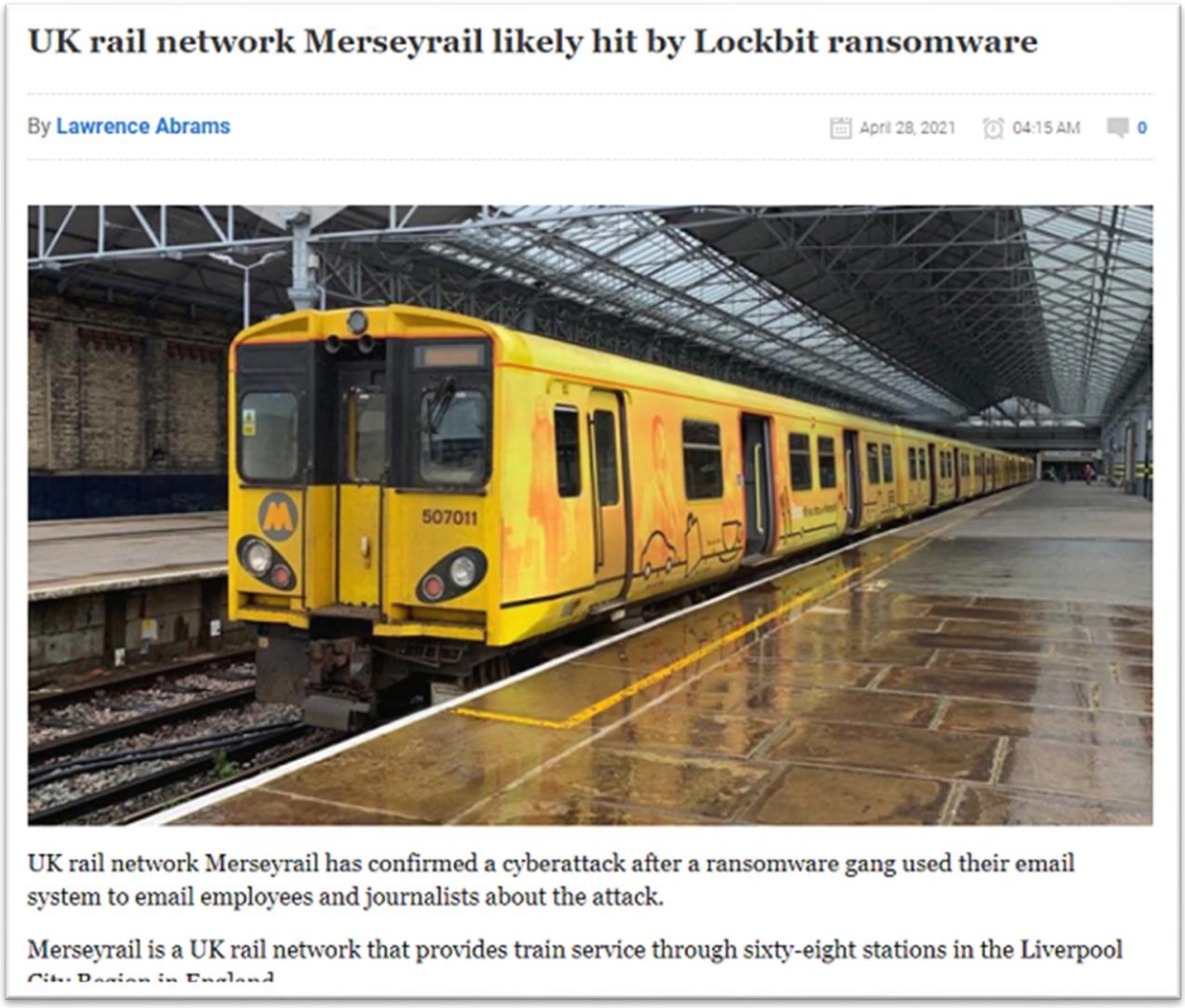
根据总部位于以色列的网络安全公司 Cyberint的研究人员的说法，LockBit勒索软件利用通过鱼叉式网络钓鱼电子邮件收集的凭据，或尝试连接到通过疯狂攻击而暴露的Windows远程桌面以进行入侵。此外，它还会利用系统中的已知漏洞。据澳大利亚网络安全中心（ACSC）称，最近它利用了Fortinet Fortios和FortiProxy产品的漏洞（CVE-2018-13379）。

Lockbit勒索软件使用网络扫描器来识别网络结构并找到目标域控制器。之后，会使用Process Hacker和PC Hunter等普通工具终止系统的进程和服务。连接到域控制器时，创建新的组策略，以在网络上的所有设备上禁用Windows Defender，并分发和运行LockBit二进制文件。LockBit勒索软件的运营商自夸称，截至2021年8月2日，它在知名的勒索软件中拥有最快的加密速度。

主要受害事例

1. 攻击英国铁路网“Merseyrail”

据美国IT安全媒体BleppingComputer报道，在2021年4月，英国铁路网Merseyrail遭到了LockBit勒索软件攻击。LockBit勒索软件运营商通过该网络管理员的电子邮件向Bleeping Computer、多家英国报社和Merseyrail员工发送了一封主题为“LockBit Ransomware Attack and Data Thef”的电子邮件，从而得知遭到了攻击。



UK rail network Merseyrail likely hit by Lockbit ransomware

By Lawrence Abrams

April 28, 2021 04:15 AM 0

UK rail network Merseyrail has confirmed a cyberattack after a ransomware gang used their email system to email employees and journalists about the attack.

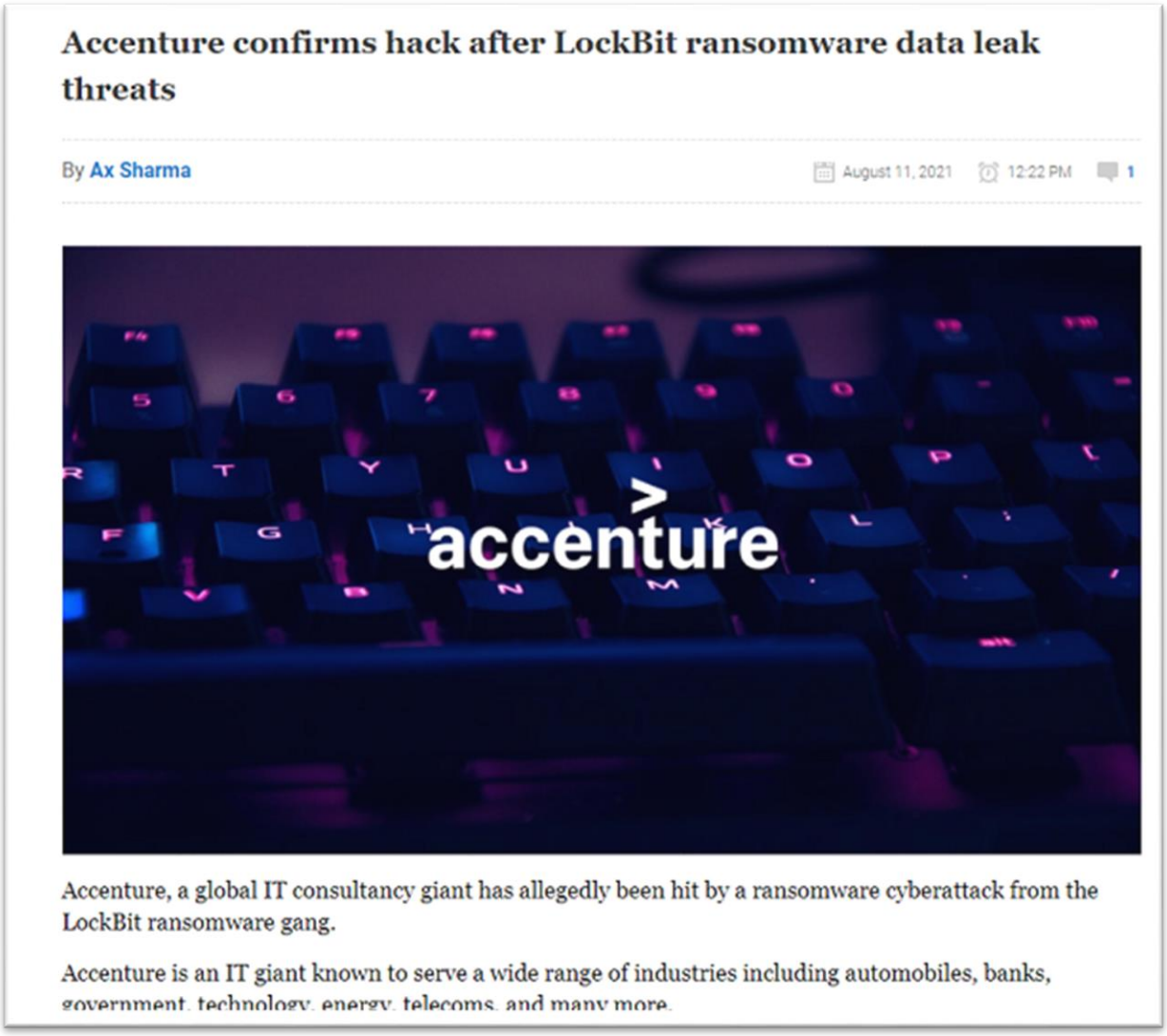
Merseyrail is a UK rail network that provides train service through sixty-eight stations in the Liverpool

【图1】英国铁路网Merseyrail遭到攻击的相关报道

2. 攻击全球IT咨询公司埃森哲（Accenture）

2021年8月，在40多个行业提供战略、咨询、数字、技术和运营服务及解决方案汽车、银行、政府、科技、能源、电信等多个行业提供服务的全球IT咨询公司埃森哲遭到LockBit勒索软件的攻击。埃森哲通过IT安全媒体BleepingComputer表示，受影响的系统已全部从备份中恢复，对业务运营没有受到影响。

然而，据网络情报公司Cyble的研究团队称，LockBit勒索软件运营商声称从Accenture窃取了6TB的数据，并要求5千万美元的赎金。他们还声称是通过Accenture的内部人员入侵了公司网络。另一家安全公司Hudson Rock表示，Accenture员工和合作伙伴拥有的2,500台计算机均受到了感染。



Accenture confirms hack after LockBit ransomware data leak threats

By Ax Sharma

August 11, 2021 12:22 PM 1

Accenture, a global IT consultancy giant has allegedly been hit by a ransomware cyberattack from the LockBit ransomware gang.

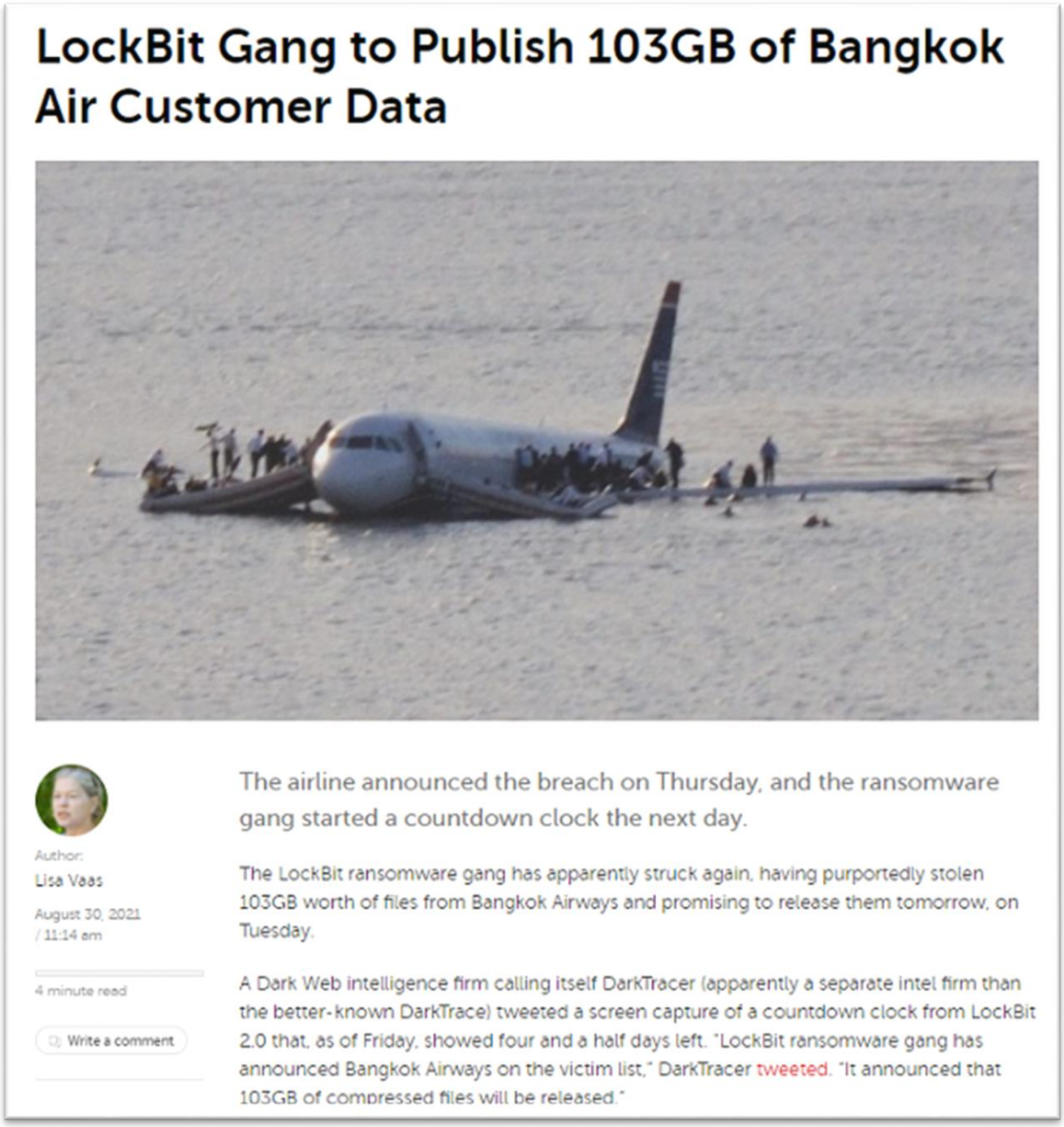
Accenture is an IT giant known to serve a wide range of industries including automobiles, banks, government, technology, energy, telecoms, and many more.

【图2】Accenture遭到攻击的相关报道

3. 攻击曼谷航空

安全公司Dark Tracer于2021年8月25日发布了一条推文，称泰国航空公司曼谷航空（Bangkok Airways）遭到了LockBit勒索软件的攻击。根据安全专业媒体Threat Post的报道，攻击者已拥有大约103GB的数据，如果不支付赎金，他们将在8月31日公开这些数据。然而，在比承诺时间提前三天的8月28日，他们突然改变了立场，并发布他们已经公开数据的公告，声称他们拥有超过200GB的数据。

曼谷航空公司 于8月26日宣布，于8月23日遭到LockBit勒索软件的攻击，导致乘客姓名、姓氏、国籍、性别、电话号码、电子邮件地址、其他联系方式、护照信息、过去的旅行历史、部分信用卡信息和特殊机内餐信息可能已被泄露。



【图3】曼谷航空遭到攻击的相关报道

4.攻击韩国企业

2021年8月23日，安全新闻报道称，一家工业橡胶制品和油封制造商以及一家食品制造商的美国子公司遭到LockBit勒索软件攻击。攻击的确切日期和损失规模等细节尚未公布，但该案例表明韩国公司也面临了LockBit勒索软件的威胁。

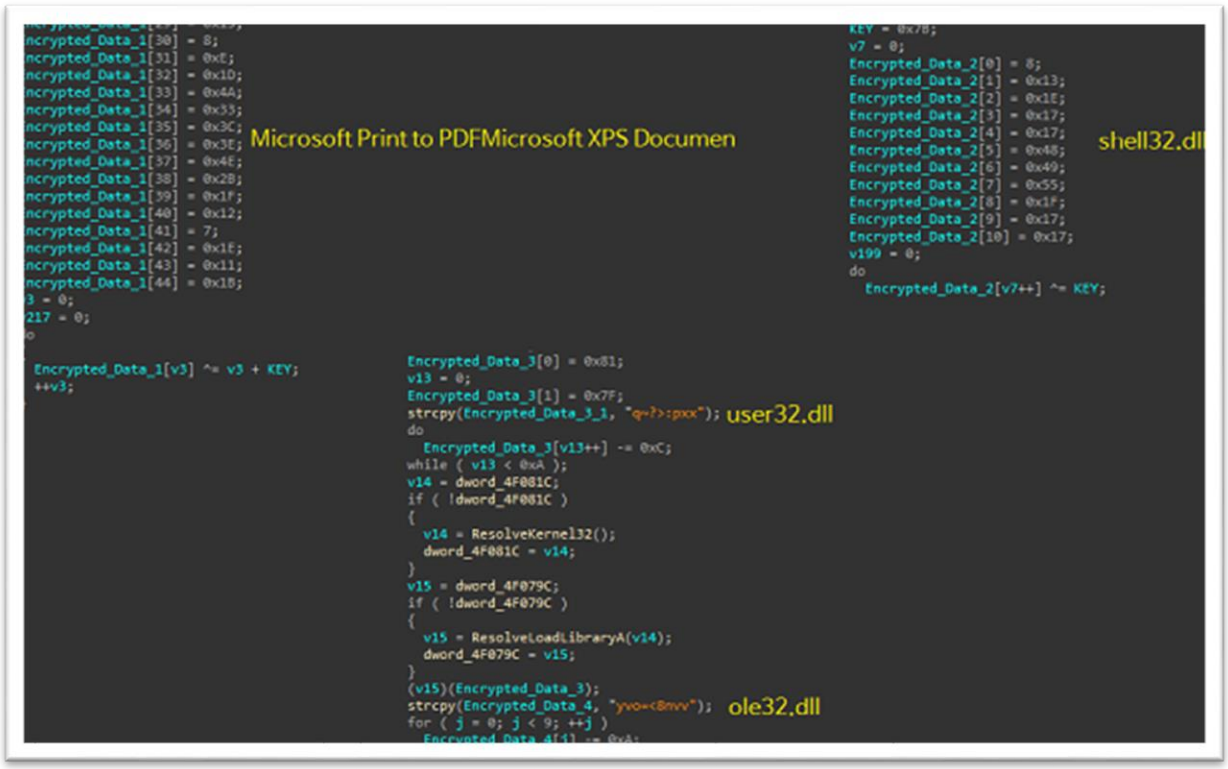
LockBit 勒索软件攻击分析

首先，AhnLab分析的Lockbit勒索软件的基本信息如下。

项目	内容
长度	959KB (985,528 bytes)
创建时间	2021年7月26日 7点34分1秒 (UTC基准)
MD5	6fc418ce9b5306b4fd97f815cc9830e5
SHA1	95838a8beb04cfe6f1ded5ecbd00bf6cf97cd564
SHA256	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049
主要功能及特点	加密文件 (LockBit Ransomware 2.0)
AhnLab诊断名	Trojan/Win.Generic.C4565305 (2021.07.25.00))

【表1】文件信息

查看分析结果，许多字符串使用不同的密钥以不同的方式（KEY）进行加密。



【图4】加密字串符

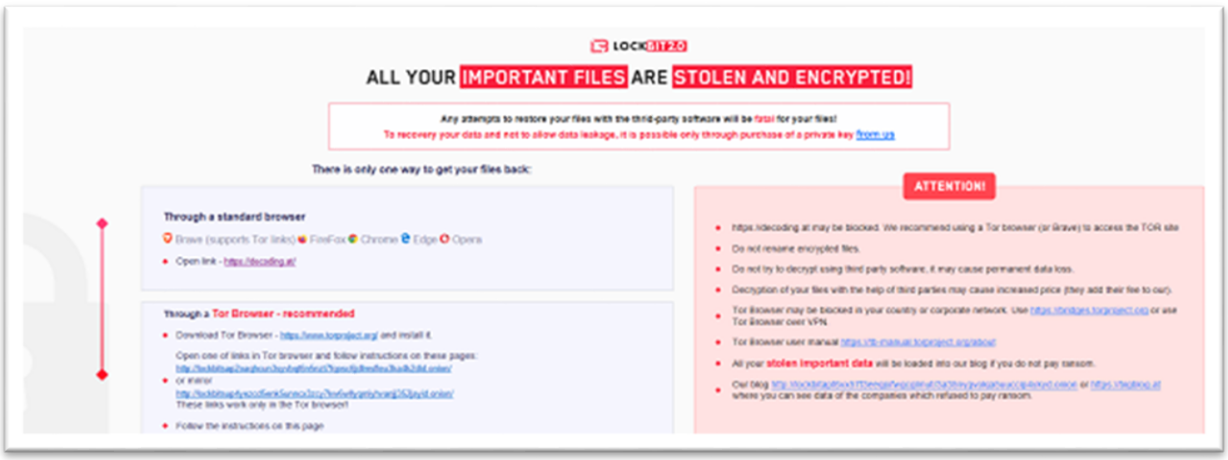
LockBit勒索软件可以使用轻量级目录访问协议（LDAP）查询Active Directory域中的连接系统。在查询字符串中，CN代表Common Name，DC代表Domain Component，该信息用于搜索其他链接的网络和系统。然后创建一个新的组策略更新，以禁用Windows Defender实时保护、提交警报样本和检测恶意文件的默认操作。最后，运行PowerShell脚本以更新刚刚在域中的所有系统上创建的组策略。

此外，它还通过删除卷影副本（Volume Shadow copy）、关闭系统恢复模式和关闭Windows错误恢复通知窗口来阻止系统恢复。

LockBit勒索软件不管在文件加密之前和之后，都会终止所有正在运行的服务与分析、防病毒软件、远程服务和相关进程。它会加密除特定文件夹、扩展名和文件之外的所有文件，并为每个加密文件名末尾添加了“.lockbit”后缀，同时还更改了所有加密文件的图标。 此外，它还会在多个文件夹中放置赎金记录。

【图5】（左）加密前（右）加密后

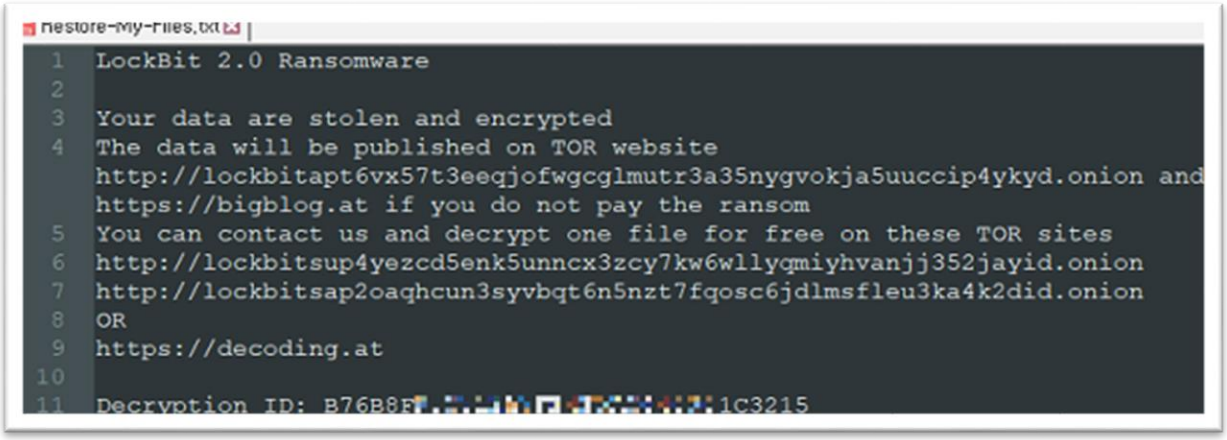
加密所有文件后，它会通过篡改桌面壁纸和使用HTA打开窗口，通知用户系统已被感染。



【图6】感染通知

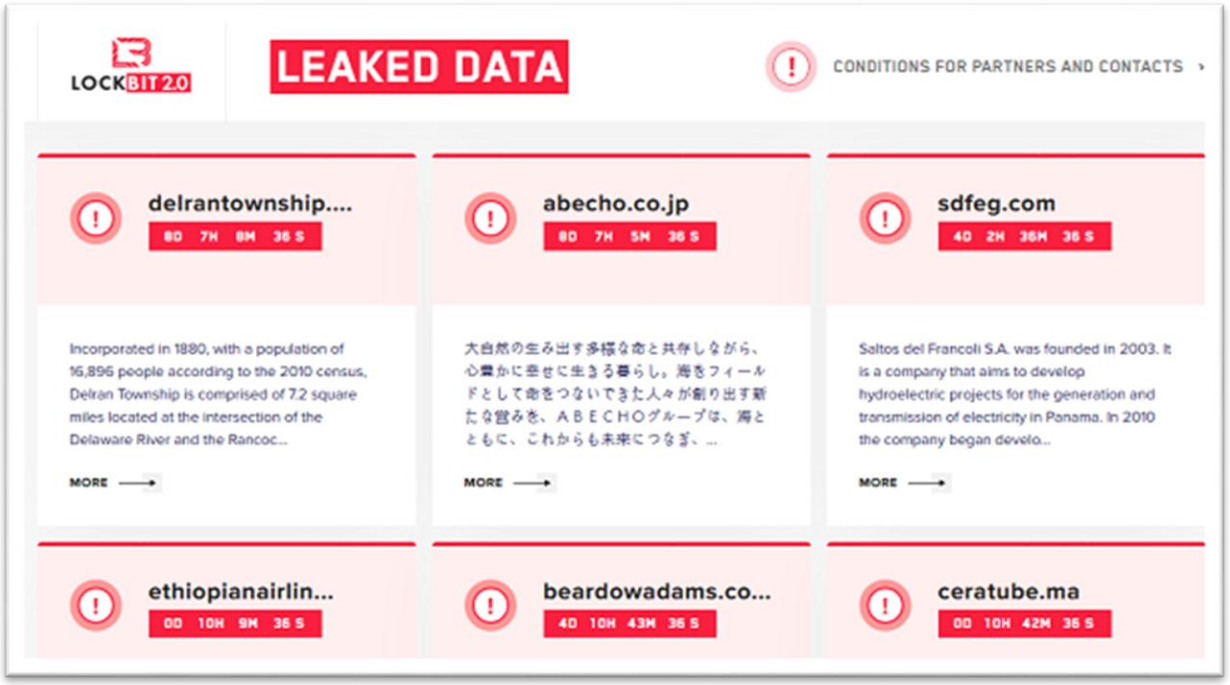
【图7】篡改桌面壁纸

它通过赎金记录诱导用户访问并解密TOR web解密网站。如果用户不支付解密费用，他们就会威胁要将数据分发到“Leaked Blog”。此外，它还通过打印机打印赎金记录，这是过去Egregor勒索软件使用的功能。



【图8】赎金记录

访问赎金记录中引导的TOR web解密网站时，网站页面上未注明解密费用，推测为通过聊天与运营商达成协议后进行解密。如果访问Leaked Blog，可以看到推测为已受害的公司主页，并通过发帖看到他们正在招募Lockbit合作伙伴。



【图9】推测为受到攻击的企业

结论

Lockbit勒索软件主要针对美国、中国、印度、印度尼西亚、乌克兰和多个欧洲国家进行了攻击。但最近，韩国企业也遭受了攻击，因此需要我们特别提高警惕。尤其是，Lockbit Ransomware 2.0版本甚至滥用AD组策略，对整个Windows域进行加密，导致更大损失。

攻击者使用通过鱼叉式网络钓鱼或疯狂攻击获得的信息进行初使攻击入侵。为了预防被这种勒索软件感染，需要遵守下面的基本安全守则：不要访问不安全的网站；避免打开来自来源不详的电子邮件和不受信任的链接；使用最新版本的防病毒软件进行定期扫描，以不断检查是否存在可疑文件或恶意代码；执行定期备份实践并将重要数据保存到另外的存储设备，如可移动硬盘。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com