INCLUDEPICTURE "http://www.venustech.com.cn/vc/img/banner0726.jpg" * MERGEFORMATINET

勒索软件应急指南

适用声明

本指南适用于企业发现受勒索软件攻击后的处理场景。

阅读对象为:

IT部门负责人安全管理员系统管理员 数据库管理员网络管理员日志管理员

上报情况

发现勒索软件后，应立即上报IT负责人，由其主导所有相关工作。

业务部门代表应当被引入，以便判断业务受影响程度及确认临时/完整恢复方案。

阻断扩散

应立即停止受感染主机的对外连接，阻止扩散。

系统管理员:

禁用受感染主机网卡;

禁用受感染主机蓝牙;

禁用受感染主机其他具备数据传输能力的链接通道;

依据网络管理员提供的主机清单，检查是否存在其他受感染主机;

设备管理员:

1. 物理断开受感染主机网络连接;

网络管理员:

1. 全网策略禁止受感染主机接入;
2. 向系统管理员提供受感染主机可以连接的主机清单;

保护现场

应立即保护现场证据及相关环境、信息，以便测试、取证、追溯。

系统管理员:

1. 确认并记录受感染主机时间及现实环境时间;
2. 确认并记录最近一次现实环境主机正常工作时间;

设备管理员:

1. 强制关停服务器;

网络管理员:

1. 依据系统管理员提供时间，提取受感染主机网络日志（流量、连接等）;

备份管理员:

1. 对受感染主机实施整机或整盘备份;
2. 准备与真实环境一致，并且隔离的镜像环境（网络环境、主机环境等），记作测试环境;
3. 准备与真实环境一致，并且隔离的、状态为未受勒索软件攻击前的镜像环境（网络环境、主机环境等），记作验证环境;
4. 准备一套新的业务环境;

确认损失

以下所有操作应在测试环境内进行。

应确认勒索软件类型、数据受损失情况，以便建立恢复方案。

备份管理员：

1. 在测试环境克隆一个受感染主机（A）并启动，提供给系统管理员；
2. 在测试环境克隆一个受感染主机（B），使用引导盘/系统启动，提供给系统管理员；
3. 确认受感染主机的最近一个有效数据恢复点；
4. 确认若需要恢复受感染主机到上一个备份点的数据损失情况，提供给IT负责人；

系统管理员：

以下操作在受感染主机（A）中进行

1. 提取被加密的文件（尽量选择小文件）；
2. 提取勒索通知文件或文字提示信息；
3. 将被加密的文件及勒索信息上传至 https://id-ransomware.malwarehunterteam.com/ 获取勒索软件信息；

以下操作在受感染主机（B）中进行

1. 确认磁盘是否被全部加密；
2. 确认文件是否被全部加密；
3. 若此主机存在数据库，与数据库管理员确认数据库可用性、完整性是否收到破坏；
4. 确认业务数据损失情况，提供给备份管理员、IT负责人；
5. 提取日志文件给日志管理员/安全管理员分析；

日志管理员/安全管理员：

1. 依据系统管理员、数据库管理员、网络管理员提供的信息及日志，判断是否存在数据泄密风险；

IT负责人

1. 与业务部门代表沟通损失情况；

恢复计划

恢复方式一般分为四类。

1. 通过备份数据恢复；
2. 通过支付赎金获取恢复工具、密钥；
3. 通过反删除工具恢复被删除数据；
4. 通过破解工具回复被加密数据；

备份管理员

1. 评估方式1所需时间、资金、成功率、数据损失率，提供给系统管理员；

系统管理员：

1. 联络攻击者获取赎金金额信息；
2. 通过搜索引擎检索同类型勒索软件攻击后支付赎金恢复的情况；
3. 评估方式2所需时间、资金、成功率、数据损失率；
4. 通过专业恢复工具在测试环境中（例：受感染主机（B））尝试恢复数据；
5. 评估方式3所需时间、资金、成功率、数据损失率；
6. 根据已获知的勒索软件类型，访问 https://www.nomoreransom.org/zh/decryption-tools.html 查询是否已有此类勒索软件解密工具；
7. 通过搜索引擎检索同类型勒索软件是否有恢复工具；

8. 评估方式4所需时间、资金、成功率、数据损失率；（评估过程可以使用《感染环境恢复》中的指引）
9. 将4种方式的对比分析报告提交至IT负责人；

IT负责人：

1. 与业务部门代表确认恢复方式及恢复计划；

感染环境恢复

若恢复计划中使用到受感染环境的数据（恢复方式1~3），则适用以下指引。

应只恢复、迁移业务所需数据，通过隔离中转的方式，将数据迁移到新的业务环境。备份管理员：

1. 在测试环境克隆一个受感染主机（C），使用引导盘/系统启动，提供给系统管理员；
2. 在验证环境克隆一套正常主机（D）并启动，提供给系统管理员；

系统管理员：

以下操作在受感染主机（C）中进行

1. 使用解密工具解密数据；

以下操作在正常主机（D）中进行

1. 将需要迁移的恢复后的业务数据通过U盘/EFSS等中转方式拷贝至主机（D）；
2. 使用同类型勒索软件专杀工具检查是否存在勒索软件；
3. 若IT负责人确认恢复数据可以使用在新业务环境，则通过U盘/EFSS等方式从主机（D）中转移数据；

IT负责人：

1. 联络业务部门代表协助确认景象环境中的业务系统可用性，数据可用性、完整性；

取证及加固

建议由专业安全团队在测试环境中分析勒索软件攻击轨迹，确认入侵方式，还原整个过程。

建议由专业安全团队对新业务环境进行安全检查，并根据取证分析报进行网络、系统、应用、管理等层面的安全加固。