FireEye

不寻常的嫌疑人

执行摘要

APT38 是个受朝鲜政府支持、有财务动机的团体，负责对金融机构执行破坏性攻击，也进行一些全球最大的网络盗窃。仅根据广泛公布的运作，该团体就已经试图窃取超过 11 亿美元。

APT38 不是简单地获取并尽快转移资金，而被认为是更类似于间谍行动，在受损的金融机构内谨慎地进行侦察，并在达到财务目标和了解内部系统之间取得平衡。

APT38 与 TEMP.Hermit 朝鲜网络间谍活动共享恶意代码和其他开发资源，尽管我们认为 APT38 的行动更全球化，也更专门针对金融领域。

至少自 2014 年以来，该组织就已经对至少 13 个不同国家的 16 个组织进行了攻击，有时是同时进行的。

自第一次观察到的活动以来，该组织的行动已经变得越来越复杂并具有破坏性。APT38 采用一种计算方法，使他们随着时间的推移不断提高战术、技术和程序 (TTP)，同时规避检测。

目录

重新评估朝鲜政府资助的活动

2018 年，我们开始对朝鲜政府支持的网络操作进行深入审查，这些操作是基于我们之前认为是 TEMP.Hermit 发起的活动，相关数据来自 Mandiant 鉴定调查、FireEye 设备、FireEye iSIGHT 情报收集，以及与“Lazarus”（又名隐形眼镜蛇）团体有关的公开报道。通过对许多受害组织的入侵进行调查，我们获得了解整个攻击流程的独特视角。通过此审查，我们将一个活动集群分离开来，以与 TEMP.Hermit 分开进行追踪。我们现在把这个受经济利益驱使的组织称为 APT38。

- APT38 是个与朝鲜网络间谍活动运营商有关联并受经济利益驱使的团体，因试图从金融机构窃取数亿美元资金并厚颜无耻地使用破坏性恶意软件而闻名。
- APT38 执行复杂的银行盗窃，其特征通常为计划时间长、长期访问被攻击的环境，然后再试图窃取资金，在复杂的操作系统环境中操作娴熟，使用定制工具，并在之后不断努力阻止调查，同时还愿意完全摧毁受攻击的机器。
- 2016 Novetta 报告详细介绍了安全供应商如何发现与 2014年索尼影视娱乐公司 (Sony Pictures Entertainment) 遭受破坏性攻击有关的工具和基础设施。这份报告详细描述了恶意软件、战术、技术和程序 (TTP)，研究人员认为这些软件与他们称为“Lazarus”的一组开发人员和操作人员有关。“Lazarus”在很大程度上已成为朝鲜激进网络行动的同义词。我们追踪了这些归因于 TEMP.Hermit 的指标和运动。
- 根据在已识别操作中所用恶意软件的相似之处，我们对归因于“Lazarus”团体和 TEMP.Hermit 有不同的确信度。随着时间的推移，这些恶意软件的相似之处发生了分化，就像目标、预期结果和 TTP 一样，几乎可以肯定的是，TEMP.Hermit 活动是由多个运营团体组成的，这些团体主要因共享恶意软件开发资源和朝鲜政府的资助而联系在一起。
- 由于 APT38 得到了朝鲜政府的支持（并代表朝鲜政府行事），我们选择将该组织归类为“APT”，而非“FIN”。这也反映出 APT38 的操作与间谍活动非常相似。
- 我们将继续酌情参考 TEMP.Hermit 和朝鲜赞助的相关活动，而非我们现在认为归因于 APT38 的明显行动。

目标和任务

根据观察到的活动，我们判断 APT38 的主要任务是针对金融机构，并操纵银行间金融系统为朝鲜政府筹集大量资金。朝鲜政府继续进行武器开发和试验之后，国际社会对其实施了越来越严厉并尖锐的制裁。尽管平壤面临越来越大的经济压力，APT38 行动的速度可反映出，朝鲜越来越不顾一切地为了追求国家利益而窃取资金。自 2015 年以来，APT38 试图从金融机构窃取数亿美元。一些已被公开由 APT38 企图的盗窃包括：

- 2015 年 12 月越南 TP 银行 (Vietnam TP Bank)
- 2016 年 2 月孟加拉国银行 (Bangladesh Bank)
- 2017 年 10 月台湾的远东国际银行 (Far Eastern International Bank)
- 2018 年 1 月 Bancomext 银行
- 2018 年 5 月智利银行 (Banco de Chile)

银行目标

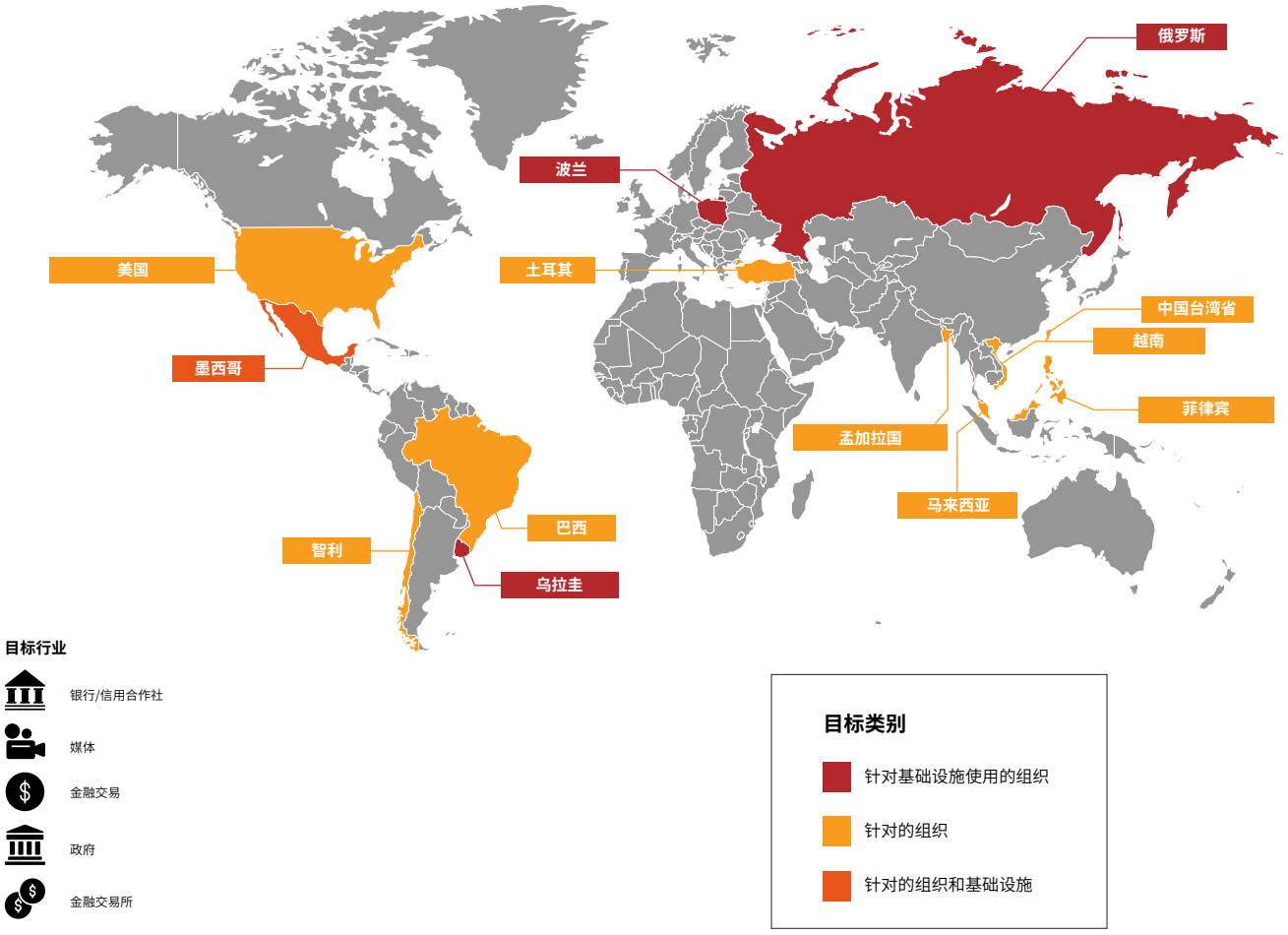
至少自 2014 年起，APT38 就一直将主要目标对准银行和金融实体[1]. 2015 年底，他们的行动升级，因为他们第一次试图进行欺诈交易。2016 年，APT38 以极快的速度实现了地域上的多样化目标。虽然 APT38 受经济利益驱动，但我们认为，在某些情况下，他们只针对实体，因为基础设施要用于协助后续操作或帮助规避检测。

在我们的审查期间，报道有多个公共事件与此活动组织有关，其主要目标是 SWIFT 系统。我们目前正在追踪与 APT38 有不同程度关联的各种可疑事件。虽然我们无法确认这些事件是由 APT38 执行的，但是根据目标的时间和位置、恶意软件以及使用的通用 TTP，我们已经观察到这些公开报告的事件和 APT38 之间有一些联系。

- 美国司法部 (DOJ) 最近于 2018 年 9 月 6 日公布的一项刑事诉讼详细说明了在另一个 TEMP.Hermit 活动中 APT38 与朝鲜政府之间的关系，在此活动中一家非洲银行似乎从 2016 年初期就已成为攻击目标。据称，该银行受到了 NESTEGG 后门程序的攻击，并涉及一起试图盗窃约 1 亿美元的案件。此案件与 APT38 使用 NESTEGG 和 APT38 在 2016 年初执行的操作大致时间重叠。
- 美国司法部的起诉书详细列出了一家东南亚银行在 2015 年末和 2016 年受到攻击。与此同时，APT38 于 2016 年全年瞄准了东南亚的组织，包括越南、马来西亚和菲律宾的实体。美国司法部的起诉书还详细列出了攻击者使用孟加拉国银行 (Bangladesh Bank)、非洲银行 (African Bank) 和东南亚银行 (Southeast Asian Bank) 之间的共享密码，证明 TTP 与 APT38 有进一步联系。
- 根据公开报道，2015 年，威胁实施者通过欺诈性的 SWIFT 交易攻击了厄瓜多尔的 Banco del Austro 银行。虽然我们对此目标的了解有限，但我们之前已经确定了 APT38 以南美实体为目标。
- 2018 年 8 月，威胁实施者利用欺诈性的 ATM 和 SWIFT 交易将目标对准了印度的宇宙银行 (Cosmos Bank)。公开的报道曾表示，有人在印度境内被利用协助收回欺诈回来的资金。虽然我们没有观察到 APT38 攻击 ATM 机，但在国家内利用个人施行攻击行为类似于公开报告的 APT38 在 SWIFT 攻击后利用个人洗钱。

1 本报告的描述是基于我们对活动的可见性和公开报告。可能还会有更多受 APT38 影响的银行和金融实体，但由于敏感性和缺乏对此类事件的公开报道，这些实体没有被公开。对未来事件的报道或调查可能扩大我们对 APT38 目标的了解。

图 1. APT38 全球目标。



其他目标

虽然该团体的主要目标似乎是银行和其他金融组织，但它们也针对各国的金融管理机构以及以金融业为重点的媒体组织。我们推测，将目标对准银行、媒体和政府机构是为了支持 APT38 的主要任务。

- 2016 年末，APT38 很可能在加密货币泡沫期间，在专注于加密货币的媒体组织中部署了战略性网络入侵（水坑攻击）。这些网站吸引了来自金融机构的大量流量，因为它们正在寻找关于不同加密货币和首次代币发行的更多信息。此事件之前曾在 TEMP.Hermit 上报道过。
- 该团体将目标对准了以商业和金融业报道闻名的新闻媒体，可能是为了帮助确定并攻击更多金融机构。这些事件之前曾在 TEMP.Hermit 上报道过。
- APT38 还有可能瞄准了金融交易所，原因可能是它们靠近银行。

图 1 显示了我们可以确认的与 APT38 目标对准的组织相关的国家地图。

图 2. 朝鲜运营商在一个地下论坛发帖。

与朝鲜政府资助的其他活动的关系

尽管美国司法部的投诉书突显了重大事件与朝鲜政府之间的潜在联系，但我们认为，这些联系让我们可以洞悉朝鲜政府实施、且不受动机或操作约束的更大规模的网络行动。该起诉书详细描述了一个复杂的网络，其中包括社交媒体帐户、基础设施、与朝鲜政府前线组织的联系、与最初侦察受害组织有关的开发人员和运营商，以及观察到的入侵行动之间恶意软件的相似之处。这些联系为在朝鲜政府指导下进行的行动提供支助，并使人们了解进行这些大规模行动所需的规模和范围。

- 美国司法部指控中提供的细节包括有关跨多个运营部门使用的电子邮件帐户和基础设施的详细信息，比如：
  - 2015 年 12 月，发现一位使用电子邮件帐户 (campbelldavid793@gmail.com) 的朝鲜运营商在地下论坛上发帖（如图 2 所示），要求“无声文档入侵”。
  - 后来发现这个电子邮件帐户向美国国防承包商发送鱼叉式网络钓鱼邮件。
  - 用于访问该电子邮件帐户的朝鲜 IP 地址也用于访问另一个帐户 (wangchung01@gmail.com)。
  - 这个电子邮件帐户与鱼叉式网络钓鱼邮件中的测试内容有关，后来在发送到孟加拉国银行的鱼叉式网络钓鱼邮件中发现了这一点。
- 美国司法部的起诉书使人们了解到，在对美国国防承包商、索尼影视娱乐公司 (Sony Pictures Entertainment) 和与他们电影 *The Interview* 有关的演员、孟加拉国银行和其他有关组织控进行侦察的操作员帐户存在重叠部分。报告指出，运营商对目标组织和与这些组织相关的个人执行了在线调查。据称，该运营商帐户向相关个人发出了领英 (LinkedIn) 邀请，随后运营商向其中许多人发送了鱼叉式网络钓鱼信息。
- 起诉书还详细列举了针对不同组织的恶意软件的相似之处。
  - 针对原告朴金浩 (Park Jin Hyok) 的指控将他与多个活动联系在一起，包括我们现在归咎于 APT38 的 SWIFT 欺诈事件，仍归因于 TEMP.Hermit 的航空航天和国防承包商受攻击事件，以及 WANNACRY 勒索软件的发布。
  - 关于这些重叠部分的具体技术说明已列于此报告的恶意软件章节。

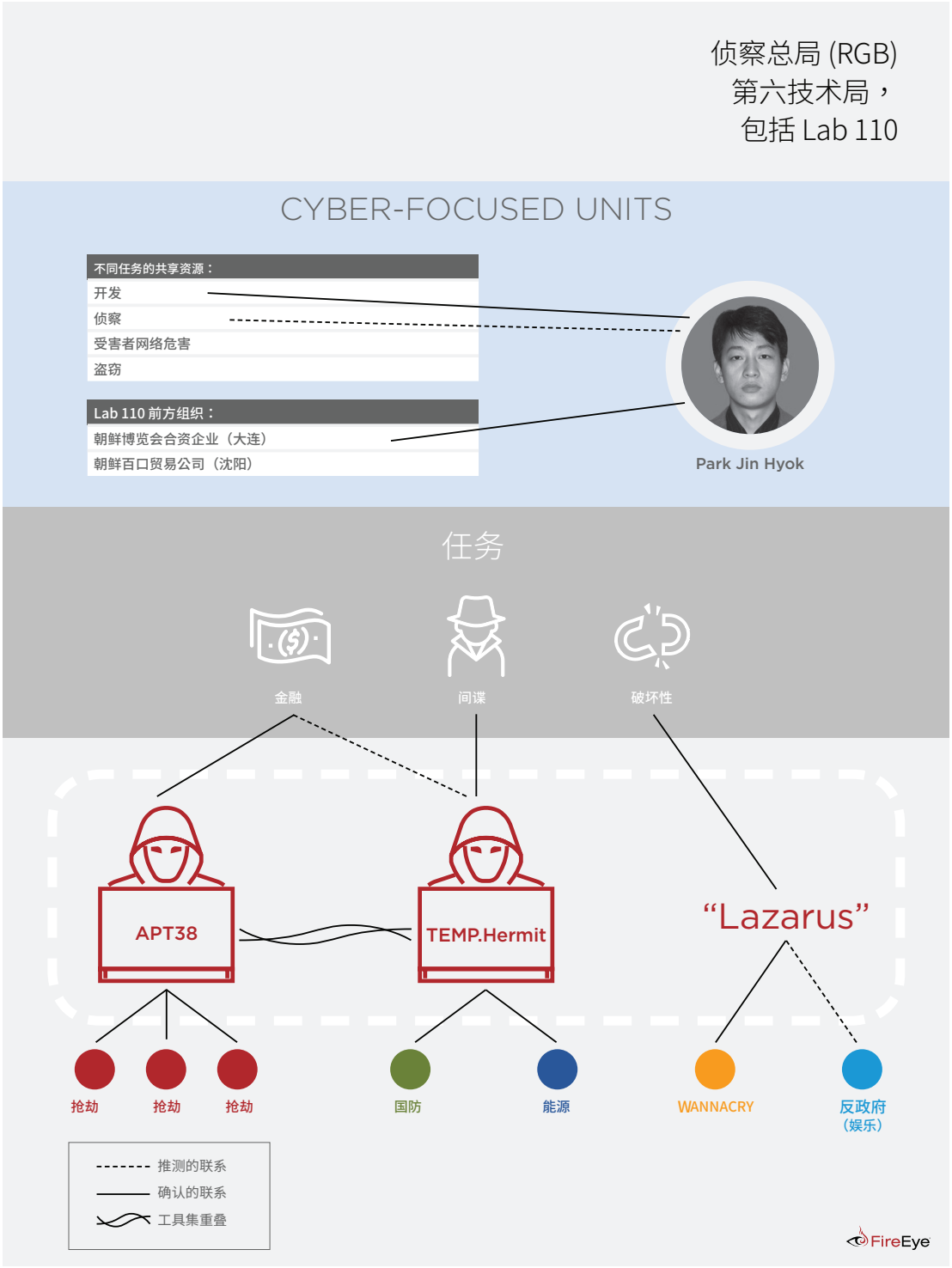
我们相信,目标同时对准娱乐、国防和金融行业的多个组织将需要大量的资源和多个团队来努力实现特定目标。

- 用于调查受影响组织的重叠帐户表明是同一个最终发起人下令对目标组织执行侦察活动。
- 最有可能的是,那些进行网络钓鱼和妥协后操作的技能组合是不同的,这些工作职能也可能是分离的。例如,在一名受攻击实体身上,起诉书中所述的与运营商有关的鱼叉式网络钓鱼和观察到的与企图盗窃有关的活动之间存在明显的时间差距,这表明鱼叉式网络钓鱼不一定是企图盗窃的同一行为人执行的。
  - 考虑到上述例子中鱼叉式网络钓鱼和盗窃活动之间的时间差,我们认为是朝鲜政府下两个独立但相关的团体负责执行任务;一个与侦察有关(TEMP.Hermit 或相关团体),另一个与盗窃有关(APT38)。
  - 另一种可能的解释是,在许多情况下,很难在受影响的金融机构确定原始入侵方法(APT38 擅长掩盖它们的踪迹),这使得鉴定分析师很难追溯操作的源头。
- 在受害组织中观察到的恶意软件的相似之处,可能表明攻击者可以访问共享的开发资源或相同的代码存储库。

APT38、TEMP.Hermit 以及其他相关事件和组织之间的联系理论上如下图 3 所示。如美国司法部的起诉书所述,朴金浩的参与很可能表明他扮演了恶意软件和/或运营开发角色,他的工作已分享给多个有不同动机的朝鲜运营实体。

- 美国司法部的起诉书中概述了朴金浩与以网络为重点的朝鲜军事单位 Lab 110 的联系及其前线组织的联系。这些联系在与朝鲜军事单位的联系部分中有进一步详细说明。
- 朴金浩的活动与多起事件有关,这些事件在公开报道中通常被描述为与“Lazarus”有广泛联系,其中包括觊觎和瞄准娱乐产业。虽然恶意软件的相似之处和共同赞助将这些事件与朴金浩联系在一起,但是 APT38 和其他相关活动集群之间存在显著的区别。
- 特别值得一提的是,APT38 之所以引人注目,是因为它特别关注金融机构和运营,试图利用 SWIFT 欺诈手段来一次性窃取数百万美元。尽管工具集有重叠,但这与 TEMP.Hermit 更为传统的间谍活动有很大不同,也不同于其他被公开称为“Lazarus”的操作。

图 3. 对 APT38 与朝鲜政府支持的其他行动的联系的概念性描述



我们可以确认，APT38 操作员的活动与朝鲜政府有关，但仍保持着一系列共同特征，包括动机、恶意软件、目标和 TTP，这些特征使其有别于其他国家支持的操作。

- APT38 的操作、恶意软件和动机与 TEMP.Hermit 不同。
  - 正如前面提到的，我们确信 APT38 的任务是将目标对准金融机构和金融系统，为朝鲜政府筹集资金。相比之下，TEMP.Hermit 是朝鲜资助的网络间谍活动集群，主要针对的是国防和政府实体；我们认为，它的任务是收集那些将有利于朝鲜利益的国家和被视为对朝鲜政府构成威胁的反对活动的战略情报。一般来说，TEMP.Hermit 的调查范围也更广，2015 年它的目标是能源研究，2017 年它的目标是电力事业。
  - 至少自 2014 年初以来，APT38 的操作几乎完全专注于开发和开展针对国际实体、受经济利益驱使的活动，而 TEMP.Hermit 的操作通常专注于韩国和美国。例如，2017 年 7 月，TEMP.Hermit 的目标是美国国防承包商，这很可能是朝鲜导弹计划和韩国导弹防御计划引发的政治冲突的结果。
- 公开报道通常报道受经济利益驱动的盗窃活动，作为“Lazarus”的子组，例如 Kaspersky 施行的“Bluenoroff”和 CrowdStrike 施行的“Stardust Chollima”。
- 此外，APT38 的工具集更加专业。恶意软件如 DYEPACK（一套操纵 SWIFT 服务器上本地数据的工具）是专门为入侵错综复杂的银行交易系统而设计的，如 SWIFT。

需要指出的是，并非所有受经济利益驱使的朝鲜活动都可归因于 APT38。

- 虽然已经观察到更大的 TEMP.Hermit 团体瞄准了与加密货币相关的其他金融相关组织，但我们的数据没有显示这些事件与 APT 38 的其他操作有基础设施、恶意软件、目标或时间方面的重叠。
- 另一个由朝鲜政府支持的团体 APT37 (Reaper) 瞄准了一家中东金融公司，但没有金融欺诈的证据。
  - 这个组织可能是 APT37 的目标，因为它从朝鲜撤出了业务运营。
  - APT37 和 APT38 的基础设施没有明显重叠，重点是针对金融机构。虽然 APT37 之前针对的是金融业，但它并不像 APT38 那样专注于窃取资金。

制裁的影响

尽管朝鲜针对特定国家的网络行动可能受外交因素的驱动，并且这种制裁被认为是对平壤的侮辱，但对朝鲜实施越来越严格、越来越多的金融制裁可能促使形成 APT38 的核心使命和操作。

- APT38 的运营始于 2014 年 2 月，并可能受到 2013 年 3 月实施的金融制裁的影响。该制裁阻止了大量现金转账，并限制朝鲜进入国际银行系统。
- 2016 年 3 月和 11 月实施的制裁扩大了限制范围，通过终止合资企业，并禁止各国在朝鲜开设新的银行分支机构，进一步限制了朝鲜进入资金和国际金融体系。在一年之内的多轮制裁可能增加了朝鲜迅速筹集资金的压力，他们在 2016 年 2 月试图进行的盗窃就表明了这一点，而就在两个月前，朝鲜在 2015 年 12 月的一次盗窃未遂。尽管在 2016 年 1 月进行了多次积极入侵，但新的制裁可能导致了 APT38 在 2016 年 10 月通过水坑攻击完成的目标升级。
- 2017 年再次实施多项制裁措施，这可能继续影响 APT38 企图盗窃的速度，制裁于 2017 年 9 月和 12 月实施，而后 2017 年 10 月和 2018 年 1 月分别出现了企图盗窃。

下面图 4 列出了与 APT38 主要企图盗窃有关的这些事件和其他重大事件的详细清单。

2 据广泛报道，朝鲜运营商对索尼影视娱乐公司 (Sony Pictures Entertainment) 的电影 The Interview 实施了破坏性攻击，因为人们认为该片直接侮辱了朝鲜政府。

图 4.
APT38 行动和朝鲜日益恶化的财政状况

战术、技术和程序

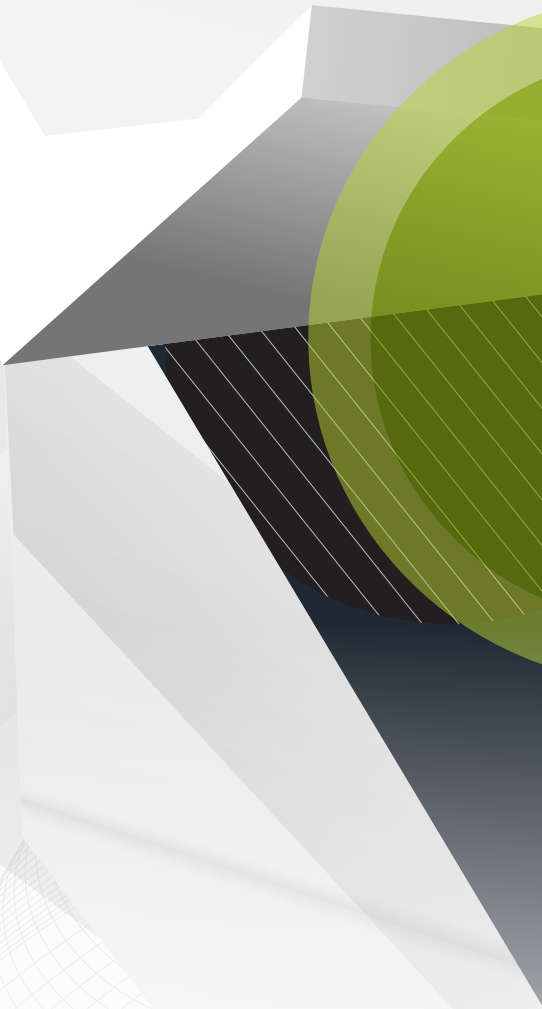
早期活动和运营开发

APT38 的早期运营表明，该团体至少在 2014 年 2 月就开始瞄准金融机构，意图操纵金融交易系统，尽管我们直到 2015 年才观察到欺诈交易。这些活动提供了一些关于学习阶段的指示，这些指示将为稍后确定 APT38 活动的 TTP 制定提供信息。

- 我们没有证据表明，在 APT38 离开被入侵的环境之前最早的目标金融机构受到了欺诈交易的影响，这可能表明 APT38 当时只是在执行侦察活动。
- 最初的行动目标很可能是东南亚的金融机构，因为朝鲜在这些国家有更多的机会进入洗钱网络。
- 2014 年初，该团体部署了 NESTEGG（后门攻击）和 KEYLIME（键盘记录）恶意软件，旨在影响一家东南亚银行的金融机构专用系统。尽管受害银行使用了 SWIFT，但没有证据表明这些工具当时被用于针对 SWIFT 系统。这些因素很可能表明 APT38 仍在学习与金融交易有关的各种系统。
- 美国司法部公布的详细信息显示，恶意软件开发人员阅读了 SWIFT 系统的用户手册，这表明他们最初在开发针对 SWIFT 的恶意软件（比如 DYEPACK）时做出了一些努力。之前观察到的 DYEPACK 是在 2015 年 12 月部署。

根据观察到的事件，我们认为 APT38 活动最初集中在东南亚，随着该团体提高自身的能力，不久之后在全球扩张。

- 瞄准东南亚市场的时间可能从 2014 年 2 月到 2017 年底。
- 2016 年初至年中，该公司开始向拉丁美洲和非洲等其他地区扩张。拉丁美洲的组织至少要到 2018 年 5 月才成为目标。
- APT38 的操作在大约 2016 年 10 月至 2017 年 10 月扩展到欧洲和北美。



操作规模

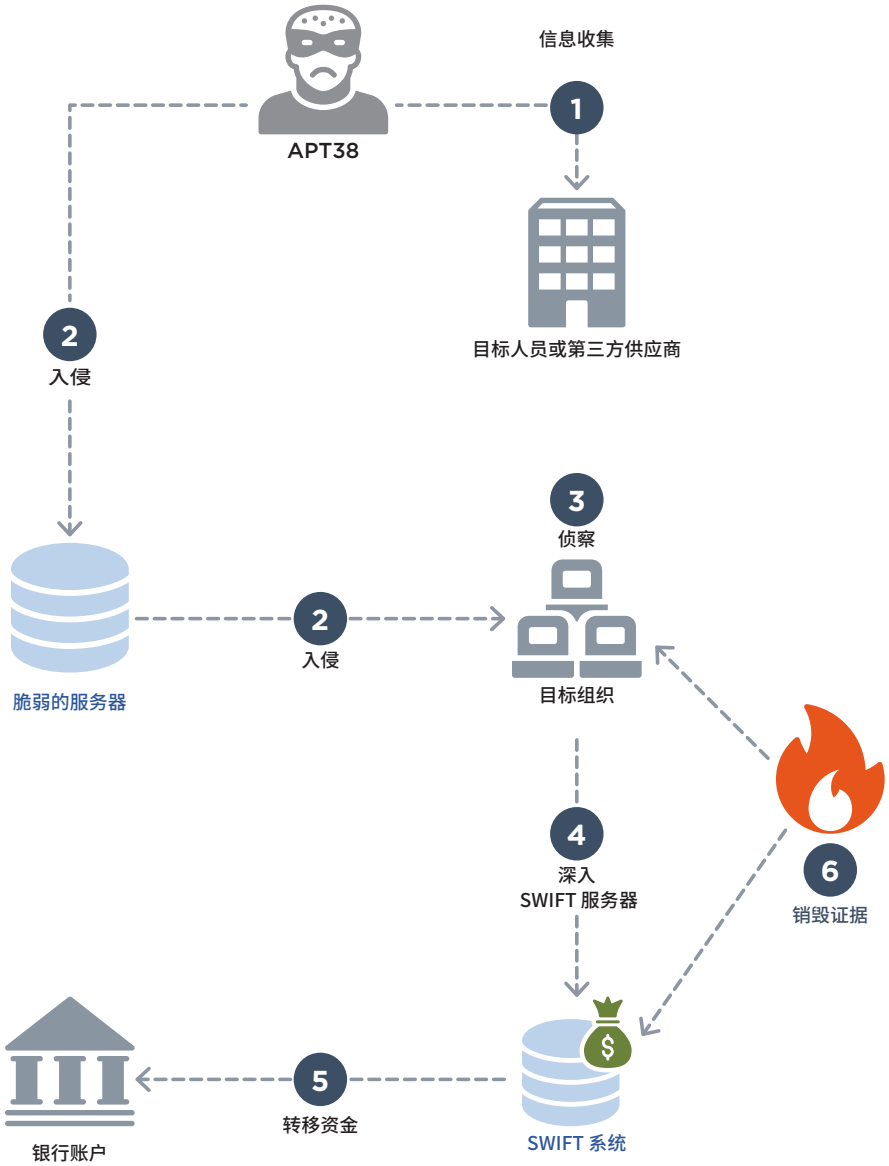
根据并发主动操作的频率和数量，一些迹象表明 APT38 是可自行支配大量资源的大型运营商。此外，APT38 似乎可以访问与 TEMP.Hermit 相关的共享资源，很可能大大增加了该团体可用人员的数量和恶意软件开发的速度。

- 从 2015 年 11 月到 2016 年底，APT38 至少参与了 9 项针对银行的独立入侵行动。这是一个团体同时执行的大量入侵行动。并发入侵行动的总数可能比这还要多，特别是考虑到金融行业以外的目标以及上文目标部分详细描述的可疑 APT38 活动时更是如此。此外，在此期间，许多操作处于攻击生命周期的不同阶段，增加了同时管理所有操作的复杂性和工作量。
- 该团体进行了极为彻底并耗时的侦察活动，表明它既有大量人员，又有大量时间来专门从事冗长的行动。例如，在多个实例中，APT38 专门花时间观察网络活动并收集可访问 SWIFT 服务器的用户和系统的关键信息。
- APT38 维护一个独有的非公共后门和其他实用程序的大型库，详细内容已列于下面的恶意软件章节中。此外，APT38 还不断改进工具，以纳入其他战术，包括规避检测的措施。例如，威胁实施者修改了 DYEPACK，以避免将恶意软件写入磁盘，方法是修改要在内联内存中使用的初始独立版本。
- 除了网络行动之外，公开报告还详细说明该团体招募了本国的人员，并与他们合作，以协助完成 APT38 盗窃活动的结尾工作，包括负责洗钱和与被盗资金接收银行进行互动的人员。这增加了复杂性和支持 APT38 操作的多个组件之间的必要协调。

现代银行盗窃概述

在较高的层次上，APT38 的目标对准金融机构，随后的盗窃尝试都遵循相同的常规模式，如图 5 所示并在下面说明。

图 5. APT38 网络银行抢劫



盗窃阶段和操作特征

1

信息收集

特征：

- 调查目标组织的人员。
- 调查目标组织可能具有 SWIFT 系统访问权限的第三方供应商，以了解 SWIFT 交易的机制。

操作细节：

根据观察到的入侵情况，我们认为该团体致力于以个人为目标，这些人员具有能够进一步访问目标组织的帐户。美国司法部公布的更多细节让我们了解到为收集信息而分配的大量时间和资源。这种信息收集可能为 APT38 活动提供支持。

- APT38 操作员曾多次试图入侵客户经理的邮箱，可能是为了调查哪些员工可以访问与 SWIFT 相关的系统。
- 美国司法部的投诉书详细介绍了针对目标的调查以及社交媒体活动，根据目标和时间重叠，这些活动可能支持 APT38 操作。
  - 至少有一次，对受害银行的侦察活动是在朝鲜 IP 地址空间进行的。本调查确定目标银行与 SWIFT 网络的连接由第三方管理，且银行员工远程连接到第三方服务器，以查看 SWIFT 信息。一个月后，APT38 通过将信息整合到恶意软件开发中来利用此信息。
  - 根据投诉书，电子邮件帐户 watsonhenny@gmail.com 被用于发出领英 (LinkedIn) 邀请，邀请对象是一家后来成为 APT38 目标的银行员工。同一个帐户拥有同一个目标银行 37 名员工的联系名单和电子邮件地址，这表明该团体在建立联系和潜在入侵媒介方面付出了更大努力。

2

初始危害

特征：

- 水坑攻击
- 搜索并入侵 Linux 服务器，例如具有 Apache Struts2 漏洞的服务器。

操作细节：

虽然并不是总能发现每个归因事件的初始入侵媒介，APT38 依赖于水坑攻击来获得对至少一些组织的初始访问权限。在至少一个实例中，APT38 实施者还利用 Apache Struts2 的一个不安全的过时版本来在目标系统上执行代码。此外，美国司法部最近的投诉书让人们对朝鲜运营商针对 APT38 目标所采取的初步入侵技术有了更深入的了解，这些技术可能已作为初步入侵的一部分被运用到目标组织中。

- 在波兰金融管理机构（Komisja Nadzoru Finansowego，简称 KNF）的网站上举办的一场水坑活动与拉丁美洲的多个额外水坑以及一个加密货币新闻页面有关。据信，这些战略性网络破坏被用于入侵多个组织，包括受害者访问该网站时被入侵的一些在欧洲和北美组织。
- 在一个受害组织中，APT38 在进入母公司之前破坏了附属组织的环境。
- 美国司法部在起诉书中公布的细节显示，朝鲜运营商在 2015 年初利用以简历为主题的诱饵文件对一家指定银行发起了鱼叉式网络钓鱼攻击。我们对此得到了进一步证实：APT38 在 2015 年末针对银行的 SWIFT 系统采取行动之前，我们确认了 TEMP.Hermit 在一家银行使用 MACKTRUCK。这项活动是值得注意的，虽然我们承认投诉书中详细列出的运营商与 APT38 共享资源和最终赞助，但我们目前没有证据将这项鱼叉式钓鱼活动归因于 APT38。

3

内部侦察

特征:

- 在目标环境中部署恶意软件,以收集凭证并映射受害者的网络拓扑。
- 使用内部工具(比如 Sysmon 和 net.exe Windows 命令行工具)来扫描系统。

操作细节:

APT38 运营商投入大量精力来了解他们的环境,并确保针对目标系统成功部署工具。该团队已经表现出有意愿保持对受害者环境的访问权限,以了解网络布局、必要的权限和系统技术,从而实现其目标。APT38 还采取措施确保在进行内部侦察时不被发现。**平均来说,我们观察到 APT38 在受害者网络中停留的时间约为 155 天,而在被侵害的受害者中停留的时间最长,为 678 天(近 2 年)**。

- APT38 与 SWIFT 系统的首次交互与所观察到的恶意交易之间的时间长度在不同操作之间存在显著差异。
  - 在一个案例中,我们观察到,在对 SWIFT 服务器进行初步侦察后不到一个月,恶意交易就发生了。
  - 在另一个案例中,我们发现 APT38 破坏了 SWIFT 系统,在进行欺诈交易前等待了近两年时间。在这两年中,APT38 维护对环境的访问权限,安装并更新了后门,并监控活动,以了解更多关于个人用户、管理员和 SWIFT 系统的信息。
  - 可能发生了其他没有观察到的 SWIFT 交互。
- 如果可能的话,该团体在其整个运营过程中使用内部工具。例如,APT38 在多个实例中利用了 Windows Sysinternals 实用程序 Sysmon 来监视系统;在另一个观察到的案例中,该团体依靠环境中已经存在的内部文件传输软件来移动和删除恶意软件。
- APT38 运营商还试图遵循受破坏系统中已经存在的命名规范,以掩盖其活动。这包括在受害者网络中模拟文件命名规范,并将这些恶意文件隐藏在合法文件中。
- 该团体非常了解被破坏的环境,至少在一个实例中,他们在其恶意软件中加入了特定于受害者环境的硬编码内部代理 IP 地址。

4

深入 SWIFT 服务器

特征:

- 在 SWIFT 系统上安装侦察恶意软件和内部网络监控工具,以进一步了解如何配置和使用 SWIFT。
- 在目标组织的 SWIFT 系统上部署主动和被动后门。

操作细节:

APT38 密切监控 SWIFT 系统,部署各种工具来观察相关的应用程序和与之交互的用户。

- APT38 展示出对被破坏环境的了解,包括为其利益在环境中利用现有的合法工具。APT38 在 SWIFT 系统上部署了 Sysmon,以了解每个组织中使用 SWIFT 的流程、服务和用户。
- APT38 在 SWIFT 系统上安装了端口监控工具 MAPMAKER。MAPMAKER 是一种侦察工具,它枚举并打印本地系统上的主动 TCP 连接。APT38 将 Sysmon 和 MAPMAKER 结合使用,以更好地了解受害者环境中 SWIFT 系统的配置和使用。
- 据知 APT38 积极地在受害者环境中测试他们的工具,以进一步了解 SWIFT 系统。据公开报道,APT38 用 DYEPACK 打印作业拦截组件的测试版本取代了合法的"nroff.exe",一款与 SWIFT 软件套件相关的打印机实用工具。APT38 允许该实用程序运行一个多小时,处理并收集有关数百条本地 SWIFT 交易消息的信息。

5 转移资金

特征：

- 部署并执行允许 APT38 插入欺诈性 SWIFT 交易及改变交易历史的恶意软件
- 将资金转移到在其他银行设立的账户，这些银行通常位于几乎没有监管的国家，从而进行洗钱。
- 通常，会启动多个交易。

操作细节：

APT38 依赖 DYEPACK（SWIFT 交易劫持框架）来启动交易，窃取资金，并隐藏受害银行任何欺诈交易的证据。该团体使用 DYEPACK 操作 SWIFT 交易记录，并隐藏恶意交易的证据，因此银行人员在查看最近的交易时并不知情。

- 在多个受害者删除欺诈性 SWIFT 消息时识别的 SQL 语句提供了 DYEPACK 如何修改交易记录的一些证据。
- 如果 DYEPACK 处理器操作一条发送到文件或打印机的 SWIFT 消息记录，它还会修改 Alliance Access Oracle SQL 数据库中的原始记录。它通过采用一系列步骤完成：
  - 首先，它将从打印作业中提取的数据序列化为适当的格式。
  - 然后调用合法的 Oracle 命令行 SQL 实用程序来更新数据库。这些更新可能删除包含 SWIFT 消息的本地记录的行，或者更新 SWIFT 消息的本地记录的正文文本。（图 6 显示用于查询 SWIFT 记录的 SQL 语句示例。）
  - 当员工查看 SWIFT 消息的本地记录时，他们会看到攻击者使用 DYEPACK 植入的伪造数据。
  - 因为这些技术直接操作 SQL 数据库，所以交易数据在 SWIFT 框架之外被更改。
- APT38 修改了他们的恶意软件，以更好地适应如何在至少一个受害组织中使用 SWIFT 的具体情况，表明该团体拥有定制开发能力。目标受害者使用合法程序 Foxit PDF 阅读器来查看 SWIFT 的消息记录，而不是依靠打印的纸质版本。为了适应这一点，APT38 更新了 DYEPACK，以修改使用 Foxit PDF 阅读器打开的 PDF 文件，消除欺诈交易的痕迹。我们将 DYEPACK 的这个变体称为 DYEPACK.FOX。
- APT38 将资金转移到另一个国家的银行，很可能是为了协助洗钱活动。公共信息报告称，用假名和虚开的账户被用来迅速将资金转移到其他账户，通常以政府账户付款、非政府组织 (NGO)、基金会和类似组织的名义转账。
  - 根据公开报道，从孟加拉国银行窃取的资金通过多笔交易被存入了四个菲律宾的银行账户和一个与斯里兰卡一家非政府组织有关的账户。进一步的报告指出，有两人涉嫌在非法赌博活动中洗钱数千万美元。在这起盗窃案中，APT38 在各自国家等待一个周末假期，从而增加对银行当局隐瞒交易的机率。
  - 使用非政府组织来转移资金也反映在另一项行动中，其中 APT38 企图将总额超过 1 亿美元的多笔交易转移到一个韩国非政府组织的韩国银行账户中。

```
select * from saaowner.appe_<date> where appe_s_umid = '<id>';
```

图 6. 请求 SWIFT 交易的 SQL 语句示例

6 销毁证据

特征：

- 使用非公开恶意软件安全地删除日志和文件。
- 部署并执行磁盘清理恶意软件，以覆盖踪迹并破坏以后的鉴定分析。
- 在该组织的系统上使用公开可用的勒索软件来延迟 SWIFT 调查并销毁剩余的活动证据。

操作细节：

APT38 的独特之处在于，它不怕积极摧毁属于其运营一部分的证据或受害者网络。与我们追踪的许多 APT 团体一样，该团体使用各种方法掩盖其踪迹，并误导调查人员。然而，APT38 也是较为厚颜无耻的团体之一，因为它不怕造成足够的损害，使整个网络无法运作。具有这种对破坏的态度可能是因为该团体不仅试图掩盖其踪迹，而且试图为洗钱活动提供掩护。

- 一些清除痕迹的功能被植入了恶意软件本身。例如，DYEPACK 能够通过删除其服务条目和调用专门用于安全删除的实用程序来卸载自身。删除文件后，它将执行一个 Windows 批处理脚本，以移除安全删除实用程序。在一个实例中，DYEPACK 被配置为在预先配置的日期自我销毁。
- APT38 部署了其他工具（包括 CLEANTOAD 和 CLOSESHAVE），这些工具是专为清除操作中使用的其他恶意软件而设计的。在多次入侵中，APT38 清除了 Windows Event 日志和 Sysmon 日志，可能是为了阻止鉴定分析。在早期入侵中，这是手工完成的，但是随着团队活动的进展，他们开发并部署了 SCRUBBRUSH，这是一个删除事件日志和预取文件的工具，并且可能尝试清除主文件表 (MFT) 记录。
- APT38 的行动表明了该团体破坏受害者运营的意图。该团体仔细识别了环境中的所有系统（以及访问这些系统所需的凭证），然后在启动大规模的清除事件之前将雨刷恶意软件推送到选定的系统。这比依靠使用自我复制来识别和清除系统的恶意软件更容易计算和耗时。此外，BOOTWRECK（APT38 使用的一种雨刷）被配置为破坏受害设备的关键部分，然后开始系统重新启动，显示出使大多数工作站和服务器脱机的意图。图 7 显示了在一个受影响的拉丁美洲组织中观察到的磁盘启动失败屏幕示例。
- APT38 中断了组织的日常运营，包括导致网站中断、电话无法拨打及重要系统无法运行。在一次报告的事故中，APT38 使近 10,000 个工作站和服务器完全无法运行，导致银行的电话服务和其他基本服务中断。

图 7. 系统被 APT38 离线攻击的示例（来源：Twitter）

恶意软件

APT38 利用了大量定制工具，几乎可以肯定地说，这表明它对大量资源有访问权限，包括一个大型开发团队。APT38 独有的一些工具包含的一些功能和代码与 TEMP.Hermit 使用的恶意软件重叠，几乎可以肯定地说，这些团队有共同的开发人员。

- 截至撰写本文时，我们已将至少 26 种独特的非公开恶意软件系列归于 APT38，并观察到该团体使用了至少两种公开可用的恶意软件系列。这个工具集包括各种后门程序、破坏性工具、隧道器和数据采集器。
- NESTEGG 和 MACKTRUCK 共享一个硬编码字节数组，尽管这未在 MACKTRUCK 中使用，而且似乎是开发的产物。
- 在 WANNACRY 和 WHITEOUT 之间共享 260 字节的功能；该特定功能为传输层安全性 (TLS) 握手生成随机选择的密码套件。

图 8 显示了 APT38 使用的所有观察到的恶意软件系列的分类，这是按攻击生命周期的各个阶段进行分类。技术附录包含每个恶意软件系列的其他详细信息。

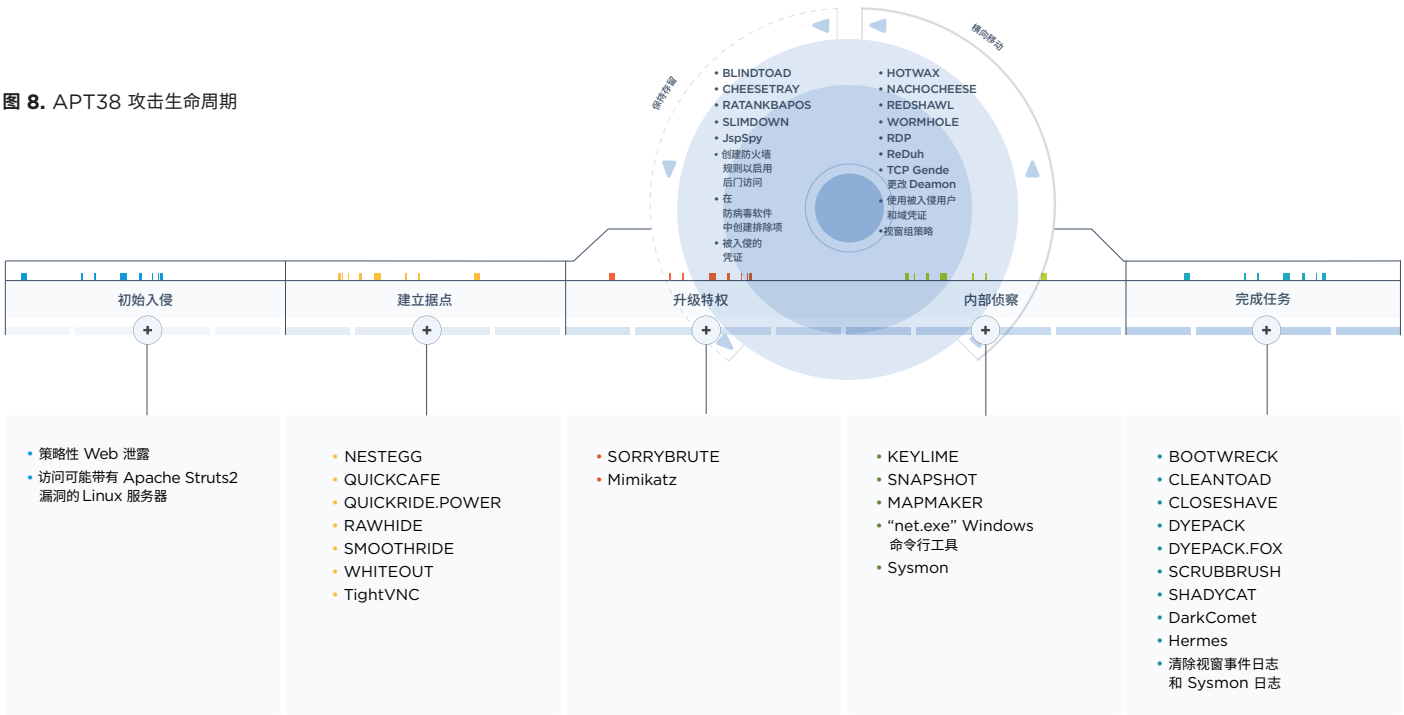


图 8. APT38 攻击生命周期

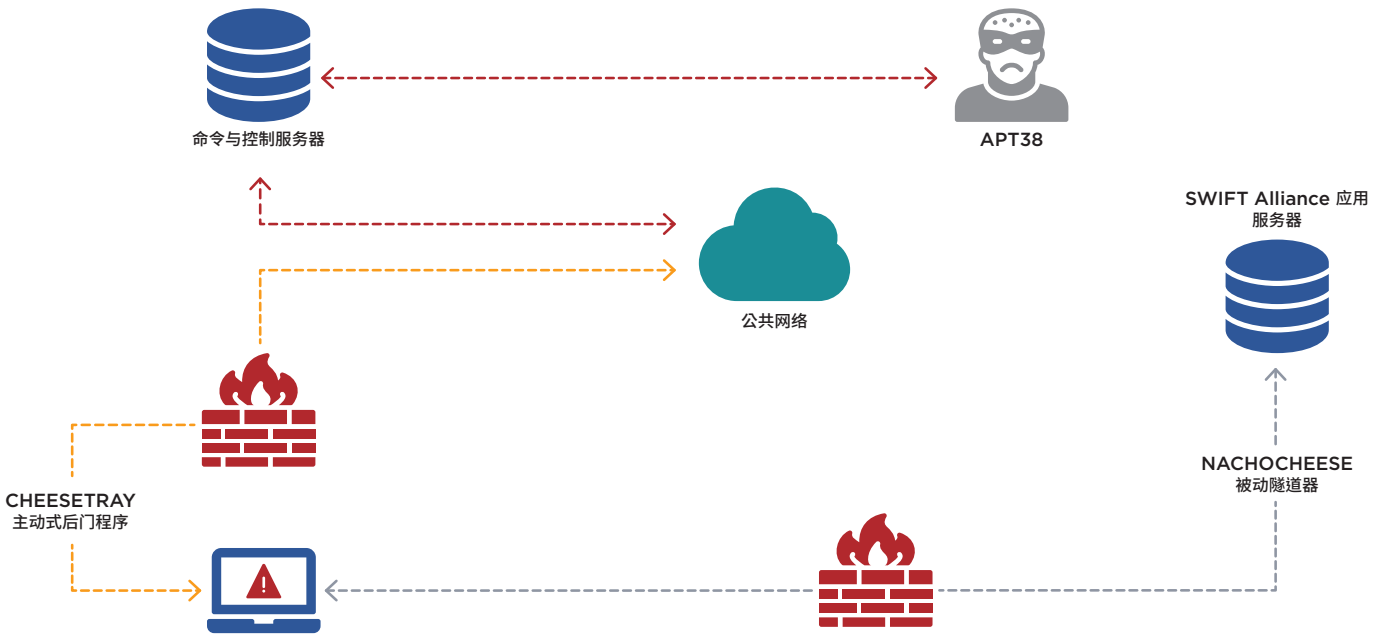
规避检测

APT38 采用了多种避免检测的技术，包括使用被动和主动后门、模块化恶意软件、主动测试和对 AV 的敏捷响应。此外，APT38 定期改变其文件的属性，以便与受害者环境中的其他文件混合

配置为以“被动”模式操作的后门表明攻击者打算通过后门从其他内部受损的系统访问该系统。APT38 始终利用“被动”后门来为分段的内部系统提供便捷的访问。

- NESTEGG 和 CHEESETRAY 后门已被识别为采用被动模式。
- 在一个受害者上，CHEESETRAY 被配置成在 SWIFT 服务器上以被动模式运行，但在 SWIFT 工作站上以主动模式运行。
- 图 9 展示了 APT38 如何使用隧道器将命令从 SWIFT 工作站上的主动 CHEESETRAY 后门传送到 SWIFT Alliance 应用服务器上端口 8443 上的主动 CHEESETRAY 后门监听。

图 9. 主动与被动后门



避开防病毒软件

APT38 使用了几种方法来规避防病毒软件并阻止调查员分析，包括使用多种代码打包方法以及对系统和注册表上的文件进行加密。

- 在 APT38 使用的 26 个独特的定制恶意软件系列中，至少有 9 个恶意软件系列使用公开可用的代码打包方法，如 Themida、Enigma、VMProtect 和 Obsidium。
- 当 APT38 的后门被防病毒软件检测到时，其反应迅速。在一个受害者网络中，一个防病毒程序开始识别 BLINDTOAD 加载器，随后在多个系统上检测到它。作为回应，APT38 运营商返回到环境中，安装了新的、未检测版本的 BLINDTOAD 和 CHEESETRAY。
- 在一个示例中，该团队故意在受害者系统上运行防病毒扫描，可能是为了确定其后门是否被检测到。

模块化恶意软件

APT38 使用的一些工具是由多个组件组成的，这些组件相互加载，并被放置在受攻击环境中的不同位置。模块化组件的使用在可扩展性方面很有用，因为程序员很容易在未来构建其他功能，而组件间功能的分布有助于规避检测。

- 例如，DYEPACK 由独立的处理器、侦听器和加密的配置组件组成。
- BLINDTOAD 是另一个 APT38 工具，它提供了一个框架来加载加密的资源，在内存中将其解码并执行。这通常绕过传统的防病毒检测。

使用假标记

APT38 在其行动中加入了一些假标记，以进一步误导调查人员，包括：

- 在一个案例中，APT38 在其操作结束时留下了 DARKCOMET 的一个变体（公开可用的后门）。这个示例的配置命令和控制 (C&C) 服务器是非洲的一家合法银行。我们推测 APT38 可能使用此工具来分散调查人员的注意力。
- APT38 还部署了 HERMES 勒索软件，该软件已被其他有财务动机的网络犯罪团伙使用。在这种情况下，勒索软件没有正确配置来收取赎金。我们怀疑这是 APT38 采用的另一种技术，用来分散调查人员注意力并销毁证据。
- 此外，APT38 所使用的 NACHOCHEESE 恶意软件含有翻译不佳的俄语字符串，这些字符串可能会误导调查人员。

归因

朝鲜基础设施

我们将 APT38 归因于朝鲜政府支持的运营商，其依据是将该活动与平壤联系起来的技术指示，以及美国司法部公布的朝鲜人士朴金浩 (Park Jin Hyok) 参与犯罪阴谋的细节。我们非常有信心地确定这些活动是由朝鲜政府指导和赞助的。由于朝鲜政府对该国的通信和互联网基础设施保持严格控制，这些行动在没有政府知情或明确支持的情况下进行是极不可能执行的。

- 美国司法部的起诉书还详细列出了朴金浩在 APT38 和其他朝鲜行动中使用的两组 IP 地址：

表 1. 朝鲜的 IP 地址范围

朝鲜的 IP 地址范围	描述
175.45.176.0 – 175.45.179.255	注册到平壤一家公司的 IP 范围
210.52.109.0 – 210.52.109.255	注册到位于中国、但租用给朝鲜的一家公司的 IP 范围

- 第三方报告证实了 APT38 在其行动中使用这些范围：
  - Group-IB 的公开报告指出 APT38 使用了相同朝鲜 IP 范围内的两个 IP（210.52.109.22 和 175.45.178.222）登录到与 (brou.com[.]uy, cnbv.gob[.]mx knf.gov[.]pl) 相关的水坑域。
  - Kaspersky 的报告表明 APT38 还在 2017 年 1 月登录到了 Apache Tomcat 服务器，该服务器用于在相同的 IP 范围 (175.45.176.0 -175.45.179.255) 内托管其恶意文件。
- 正如美国司法部在起诉书中详细描述的那样，一款来自 APT38 的 WHITEOUT（又名 Contopee）恶意软件在 2015 年至 2016 年期间对一家东南亚银行进行了攻击。该示例使用了特定的 DDNS 域 onlink.epac[.]to，这是由 DDNS 供应商的一个帐户管理。于 2015 年 10 月 6 日从一个朝鲜 IP 地址访问同一帐户。
- 如司法部投诉书所述，朝鲜运营商对东南亚银行执行了侦察，包括访问其网站，调查 SWIFT 系统用来识别银行的业务标识符代码 (BIC)，并调查相应银行执行预期欺诈性交易所需的 BIC 代码。这证明了朝鲜运营商和 APT38 有共同的动机和意图 - 即以 SWIFT 系统为目标，朝鲜运营商执行侦察，APT38 后来又以该组织为目标。

共享资源，动机

APT38 和 TEMP.Hermit 之间存在恶意软件重叠，突出显示了与朝鲜政府资助的活动相关的多个运营团体可以访问共享开发资源。虽然这些是针对不同目标的完全不同的操作，并且依赖于不同的 TTP，但是所使用的恶意软件工具要么是重叠的，要么显示共享特征（表示来自相同的开发人员），要么可以访问相同的代码存储库。虽然 APT38 不同于其他 TEMP.Hermit 活动，但这两个团体的运作始终符合朝鲜政府的利益。

- 恶意软件的相似之处（包括代码重叠和共享功能）是 APT38 和其他仍归于 TEMP.Hermit 的操作之间的主要联系。有关恶意软件相似的详细信息，请参阅前一章节。
- APT38 针对银行和其他金融机构的攻击力度越来越大，与此同时，朝鲜的财务状况不断恶化（图 4）。同样，针对美国国防承包商、韩国政府办公室及公司的 TEMP.Hermit 运动也与朝鲜的其他目标保持一致。

与朝鲜军队的联系

根据美国司法部对朝鲜程序员朴金浩的投诉书中公布的细节，我们知道 APT38 和其他与 TEMP.Hermit 有关的网络运营商与 Lab 110 有关联，Lab 110 是朝鲜侦察总局 (RGB) 第六技术局下属或同义的组织。据信，该组织利用前沿组织掩盖其活动，包括入侵网络和收集情报。这些关系如图 3 所示。

- 美国司法部的投诉书和开源报告称，Lab 110 运营通常位于中国东北的幌子公司。确定的幌子公司包括大连的朝鲜世博会合资企业 (Chosun Expo Joint Venture) 和沈阳的朝鲜白口贸易公司 (Chosun Baeksul Trading Company)。
- 第一手资料、一家外国调查机构提供的信息，以及用来访问该公司网站和相关帐户的常用 IP 地址，同时与朝鲜往来，这些都证实了有关朝鲜世博会合资企业是平壤当局经营的幌子公司。
- 据报道，类似的单位在世界其他地区也有业务，包括东南亚、东欧和中国的其他地区。
- 据信，恶意软件开发人员和其他对手是从朝鲜的大学招募而来，并直接进入 Lab 110 等军事单位工作。据报道，为这些单位提供人员的学校包括金泽克理工大学 (Kim Chaek University of Technology) 和金日成军事科学大学 (Kim Il Sung Military Science University)。

图 10. 朝鲜世博会合资企业的存档网站（来源：archive.fo）

前景和影响

APT38 目标对准金融机构很可能是朝鲜政府为支撑其受到严厉制裁的经济而做出的努力。更严格和更有针对性的制裁(从限制进入国际银行系统扩大到集中于具体的出口)很可能大大增加了压力,使业务运营更加大胆。公开报道表明,朝鲜此前从事过走私和毒品贸易等非法活动,目的是为了提高汇率并维持经济运转。我们判定 APT38 的网络盗窃是这些非法活动的延伸。从朝鲜叛逃者发布的报告那里我们还可以了解到有关以网络为中心的军事单位的详细信息,这些单位的任务是为朝鲜政府创造收入,方法通常是参与各种网络犯罪计划,包括盗版和自由编程工作。

虽然尚不清楚 APT38 的运营将如何受到美国司法部近期投诉的影响,但值得注意的是,朝鲜运营商过去似乎并未受到公开报道的影响。此外,最近 APT38 行动的时间表明,即使外交上的重新接触也不会促使朝鲜控制其有财务动机的非法活动。考虑到其过去几年致力于入侵目标组织和窃取资金的庞大资源和网络,我们认为 APT38 的运营将在未来继续下去。特别值得一提的是,由于近年来被最终阻挠的 SWIFT 盗窃事件的数量上升,再加上人们对金融信息系统的安全意识日益增强,可能会促使 APT38 采取新的策略来获得资金,尤其在朝鲜获得货币的渠道继续恶化的情况下更是如此。

技术附录: APT38 使用的恶意软件

表 2. APT38 使用的恶意软件。

恶意软件	描述	被检测为
BLINDTOAD	BLINDTOAD 是 64 位服务 DLL，可以从磁盘上加载加密文件并在内存中执行。	• FE_APT_BLINDTOAD • FE_APT_FIN_BLINDTOAD_1 • FE_APT_FIN_BLINDTOAD_2 • FE_APT_Loader_Win64_BLINDTOAD_1
BOOTWRECK	BOOTWRECK 是一个主启动记录雨刷恶意软件。	• FE_APT_Wiper_Win32_BOOTWRECK_1
CHEESETRAY	CHEESETRAY 是一个复杂的代理支持后门，可以根据传递的命令行参数以主动和被动模式运行。后门能够枚举文件和进程、驱动程序、远程桌面会话、上传和下载文件、创建和终止进程、删除文件、创建反向 Shell、充当代理服务器以及劫持进程等功能。后门在 TCP 上使用定制的二进制协议与其 C&C 服务器通信，同时将端口指定为命令行参数。	• FE_APT_Backdoor_Win64_CHEESETRAY_1 • FE_APT_Backdoor_Win_CHEESETRAY_1 • APT.Backdoor.Win.CHEESETRAY
CLEANTOAD	CLEANTOAD 是一个中断工具，它将删除文件系统工件（包括与 BLINDTOAD 相关的工件），并在从配置文件获得日期后运行。恶意软件将 shellcode 注入 notepad.exe，然后覆盖和删除文件，修改注册表项，删除服务，并清除 Windows 事件日志。	• FE_APT_HackTool_Win_CLEANTOAD_1
CLOSESHAVE	CLOSESHAVE 是安全删除实用程序，它需要一个命令行参数，该参数是到系统上现有文件的路径。它用空字节覆盖文件，更改文件名，并删除文件。	• FE_APT_Hacktool_CLOSESHAVE

表 2. APT38 使用的恶意软件。

恶意软件	描述	被检测为
DarkComet	DarkComet 是个公开可用的远程访问木马 (RAT)，具有超过 60 个不同的功能，包括收集系统信息，控制目前在受感染系统上运行的所有进程，查看和修改注册表，创建反向 Shell，修改或添加启动流程和服务，键盘记录，偷窃凭证，记录音频，扫描网络，锁定，重新启动和关闭受感染系统，用新的命令和控制 (C&C) 服务器或新功能更新恶意软件，以及下载、修改和上传文件。	• Backdoor.DarkComet Trojan.DarkComet • Backdoor.Fynloski • Trojan.Fynloski
DYEPACK	DYEPACK 是个恶意软件套件，操纵有关 SWIFT 交易活动的本地信息。DYEPACK 很可能被用来掩盖通过其他工具或策略执行的欺诈性 SWIFT 交易的痕迹。这种恶意软件的变体可能被用于部署在多个金融机构中，这些机构可能是相关恶意活动的目标。然而，它的实际部署并没有在所有这些情况下得到证实。	• Hacktool.APT.DYEPACK
DYEPACK.FOX	DYEPACK 实用程序的变体。DYEPACK.FOX 能够操纵包含 SWIFT 消息记录的 PDF 文档。	• Hacktool.APT.DYEPACK
HERMES	HERMES 是个多线程的勒索软件，它枚举系统上的所有逻辑驱动，并为每个驱动启动一个新的加密线程。它试图使用 AES256 加密所有文件，为 GetFileAttributes 请求返回 FILE_ATTRIBUTE_NORMAL。HERMES 将尝试在桌面上创建并显示一个名为 DECRYPT_INFORMATION.txt 的文件，该文件包含赎金指令。	• FE_APT_Ransomware_HERMES_1 • FE_APT_Ransomware_Win_HERMES_1 • FE_APT_FIN_Ransomware_HERMES • FE_Ransomware_Win32_HERMES_1 • Ransomware.Hermes.DNS • Ransomware.Hermes • RansomDownloader.Hermes
HOTWAX	HOTWAX 是一个模块，在启动时导入所有必要的系统 API 功能，并搜索 .CHM 文件。HOTWAX 使用 Spritz 算法以及硬编码密钥为有效内容解密，然后搜索目标进程，并尝试将解密的有效内容模块从 CHM 文件注入到目标进程的地址空间。	• FE_APT_Trojan_Win64_HOTWAX_1
JspSpy	JspSpy 是在 github.com 上公开发布的可用 web shell。公开可用的版本是“Code By Ninty”	• FE_Webshell_JSP_JSPSPY_1 • FE_Webshell_Java_JSPSPY_1 • Webshell.JSP.JSPSPY • JSPSPY WEBSHELL
KEYLIME	KEYLIME 是键盘记录器和剪贴板记录器，它将结果编码到日志文件中。	• FE_Hacktool_KEYLIME • FE_APT_Trojan_KEYLIME • FE_Trojan_KEYLIME
MAPMAKER	MAPMAKER 是一种侦察工具，它枚举并打印本地系统上的主动 TCP 连接。它查询操作系统的 IPv4 TCP 连接表，并将“<ip>:<port> -> <ip>:<port>”这样的行写入日志文件。	• FE_APT_HackTool_Win32_MAPMAKER_1
NACHOCHEESE	NACHOCHEESE 是命令行隧道器，它通过命令行接受带分隔的 C&C IP 或域，并给予攻击者对受害者系统的 shell 访问权限。	• FE_APT_FIN_Trojan_NACHOCHEESE • FE_APT_FIN_Backdoor_NACHOCHEESE
NESTEGG	NESTEGG 是内存专用的后门，可以使用自定义路由方案将命令代理给其他受影响的系统。它接受上传和下载文件、列出和删除文件、列出和终止进程以及启动进程的命令。NESTEGG 还创建了 Windows 防火墙规则，允许后门绑定到指定的端口号，以允许入站流量。	• FE_APT_Backdoor_NESTEGG • FE_APT_Backdoor_NESTEGG_2 • FE_APT_Backdoor_NESTEGG_3 • FE_Backdoor_NestEgg_DLL

表 2. APT38 使用的恶意软件。

恶意软件	描述	被检测为
QUICKCAFE	QUICKCAFE 是针对 QUICKRIDE.POWER 的已加密 JavaScript 下载程序，其利用 ActiveX M2Soft 漏洞。使用 JavaScript 混淆器混淆 QUICKCAFE。	• FE_APT_Downloader_JS_QUICKCAFE_1
QUICKRIDE	QUICKRIDE 是利用启动文件夹建立持久性的后门。它使用 HTTPS 和静态 HTTP 用户代理字符串与 C&C 服务器通信。QUICKRIDE 能够收集有关系统的信息、下载和加载可执行文件以及卸载自身。它用于攻击波兰的银行。	• Backdoor.APT.QUICKRIDE
QUICKRIDE.POWER	QUICKRIDE.POWER 是 QUICKRIDE 后门的 PowerShell 变体。它的有效内容通常被保存至 C:\windows\temp\	• FE_APT_Backdoor_PS1_QUICKRIDE_1 • FE_APT_Backdoor_PS1_QUICKRIDE_2
RATANKBAPOS	RatankbaPOS 是目标对准支付卡应用平台程序的后门，清除 track2 数据，然后将其发送至远程 C&C。RATANKBAPOS 也能运行任意命令并删除自身。该工具与 APT38 归因的基础设施相链接，这表明该组织可能考虑过用于拦截交易数据的其他策略。	• Trojan.POS.RatankbaPOS • Trojan.RatankbaPOS
RAWHIDE	RAWHIDE 是 ProcessHider Rootkit 的变体。ProcessHider 是一种后开发工具，它隐藏进程，避开任务管理器和进程管理器等监控工具。	• FE_HACKTOOL_RAWHIDE • Exploit.APT.RAWHIDE
REDSHAWL	REDSHAWL 是会话劫持实用程序，当另一位用户目前通过命令行登录到同一系统时启动一个新进程。	• FE_APT_HackTool_Win64_REDSHAWL_1
SCRUBBRUSH	SCRUBBRUSH 是中断实用程序，可以删除事件日志，预取文件，并可能试图清除 MFT 文件记录。	• FE_APT_Tool_Win32_SCRUBBRUSH_1
SHADYCAT	SHADYCAT 是 HERMES 2.1 RANSOMWARE 激进版本的植入和散布组件。	• FE_APT_Dropper_SHADYCAT_1 • FE_APT_FIN_Trojan_SHADYCAT_Dropper
SLIMDOWN	SLIMDOWN 是下载程序，通过定制加密的二进制协议获取 PE 可执行文件。	• FE_APT_Backdoor_SLIMDOWN
SMOOTHRIDE	SMOOTHRIDE 是一个 Flash 加载器，其中包含三个不同的入侵。 SMOOTHRIDE 是入侵调度程序，并根据受影响的操作系统提供三种入侵程序（CVE-2016-4119、CVE-2016-1019 或 CVE-2015-8651）。 已经观察到通过水坑运送 SMOOTHRIDE。	• Trojan.SMOOTHRIDE.Profiler
SORRYBRUTE	SORRYBRUTE 是 SMB 暴力破解工具，其接受要尝试的目标 IP、用户名和密码，以及命令行上的运行时参数，并用于横向移动	• FE_APT_HackTool_Win32_SORRYBRUTE_1
WHITEOUT	WHITEOUT 是支持代理的后门，它使用自定义加密的二进制协议进行通信。它可以使用注册表来存储可选的配置数据。经观察，后门支持 26 个命令，包括目录遍历、文件系统操作、数据归档和传输以及命令执行。	• FE_APT_Backdoor_WHITEOUT
WORMHOLE	WORMHOLE 是 TCP 隧道器，可以从 C&C 服务器动态配置，并可与其他的远程计算机端点进行中继通信。	• FE_APT_Tunneler_Win32_WORMHOLE_1

若要了解更多关于 FireEye 的信息，请访问：**www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

关于 FireEye, Inc.

FireEye 是一家情报主导型安全企业。FireEye 为客户提供无缝式、可扩展的客户安全解决方案，提供一个将创新型安全技术、国家级威胁情报以及闻名于世的 Mandiant® 咨询集成于一体的平台。通过这种方式，FireEye 为殚精竭虑防备、阻止和应对网络攻击的组织，消除了网络安全的复杂性和负担。