13

WORM AGENT

Make a* minomushi*, or worm agent (aka insider threat), out of an enemy.

A minomushi *is someone who serves the enemy but is made a ninja working for your side. Thus the agent is exactly like a worm in the enemy's stomach, which eats its belly from the inside out.*
—Bansenshūkai, Yo-nin I[1]

Never short on evocative imagery, *Bansenshūkai* describes an open-disguise infiltration technique called "the art of a worm in your stomach" (or "worm agent"), which calls for shinobi to recruit enemy insiders to perform tasks on their behalf. Such recruitment took high emotional intelligence. Shinobi had to choose an appropriate target; engineer opportunities to approach the target; and discreetly parse what the target thought about their employer, personal worth, and secret ambitions.[2] The scroll warns that candidate selection must be undertaken

with extreme care, because attempting to recruit the -wrong person to become a worm agent—or *minomushi*—could seriously harm a shinobi's mission. To maximize their odds of successful recruitment, shinobi developed eight archetypes of likely worm agents:[3]

- Individuals who have been unfairly or excessively punished by their current employer for prior offenses and who harbor deep-seated bitterness as a result
- People who, despite being born to privilege or having impressive abilities, are employed beneath their station, have been passed over for promotion, and resent being underutilized
- Habitual overachievers who consistently deliver good results for their employers but are rewarded with token titles, small bonuses, or insufficient raises—or with nothing at all Their contributions minimized, they believe they might have had a more fruitful career had they been hired by another employer. They further believe their organization makes stupid decisions because leadership values sycophants and politicians over loyal employees with real accomplishments.
- Smart and talented workers who do not get along with leadership. Because these people tend to garner disapproval easily and are considered annoyances, their employers give them low-level positions, lay the groundwork for constructive dismissal, and generally make them feel unwelcome.
- Experts in their field whose employers exploit their circumstances, such as loyalty oaths or family obligations, to keep them in lower positions
- Individuals whose job functions are in direct opposition to their personal identity, family needs, or beliefs, leading them to regret the work they do
- Greedy and conniving people who lack loyalty or a moral compass
- "Black sheep" employees who have a bad reputation due to past misdeeds and feel frustrated about their diminished status

After a shinobi selected a potential *minomushi*, they created a plan to become acquainted and build a relationship with the candidate. *Bansenshūkai* instructs shinobi to present themselves as rich and curry the target's favor with money; use friendly banter to discern their likes, beliefs, and sense of humor; and use light banter to surreptitiously discover their inner thoughts. If the target's character aligned with a worm agent archetype, then the shinobi attempted to exploit those *minomushi*

traits by promising wealth, recognition, and help with achieving their secret ambitions—or, more directly, alcohol and sex—in exchange for betraying their employer.[4]

Before exploiting the newly turned *minomushi*, shinobi were advised to obtain an oath of betrayal, collect collateral assets to guarantee the worm agent's loyalty, and establish signals and other operational security (OPSEC).[5]

In this chapter, we will review insider threats. We will compare and contrast the disgruntled worker with the recruited insider threat. We will also touch on the detection and deterrent methods that organizations use to deal with insider threats, as well as a new, tailored approach—, inspired by the shinobi scrolls—to proactively prevent at-risk employees from becoming insider threats. Lastly, a thought exercise will ask you to imagine which former and/or current employees could become insider threats and to examine how you have interacted with them.

Insider Threats

An *insider threat* is an employee, user, or other internal resource whose actions could harm an organization—whether intentionally or not. Because they did not intend to perform malicious actions, a hapless employee who opens a phishing email and infects their workstation with malware is an unwitting insider threat. On the other hand, a disgruntled worker who purposefully releases a virus into the organization, whether for personal reasons or on behalf of an adversary, is an intentional insider threat. Because insider threats are legitimate, authorized users with authentication, privileges, and access to information systems and data, they are some of cybersecurity's most difficult problems to mitigate.

Many organizations rely on technical controls and threat hunters for early detection of insider threats. Technical detection techniques—things like behavior heuristics—can help identify potential insider threats. Vigilant cyberdefenders and hunters may investigate users who take uncharacteristic or inappropriate actions, including downloading all files to external portable media, performing searches for sensitive or proprietary data unrelated to their job, logging in to perform nonpriority work on weekends or holidays, accessing honeypot systems and files clearly labeled as restricted access, or downloading and using hacker-like tools to perform actions outside their job functions.

But technical controls are only part of a solid defense strategy, even for mature organizations. By checking references; performing background checks, including of criminal and financial history; and

screening for drug use, the employer can verify that employees are not plainly vulnerable to undue influence. The human resources function plays a key role in identifying potential insider threats. Some human resource departments conduct annual employee surveys to identify potential issues, and others terminate at-risk employees proactively or recommend rescinding certain access privileges based on troublesome findings. Unfortunately, it is common for organizations to exercise minimal precautions. Most trust their employees, others ignore the issue, and still others accept the risk of insider threats so business operations can run smoothly.

Entities that fight insider threats more aggressively, such as organizations in the defense industry and the intelligence community, implement advanced detection and prevention measures such as polygraphs, routine clearance checks, counterintelligence programs, compartmentalization, and severe legal penalties—not to mention cutting-edge technical controls. However, even these controls cannot guarantee that the malicious actions of all insider threats—especially those assisted by sophisticated adversaries—will be detected and prevented. They also present unique implementation and operational challenges.

A New Approach to Insider Threats

Organizations that focus their efforts on scrutinizing employees and attempting to catch them in the act are waiting too long to address the threat. A more proactive approach is to foster a work environment that doesn't create the conditions in which insider threats thrive. Some of the following suggestions are tailored to remediating specific insider threat archetypes.

1. *Develop detection and mitigation techniques.* Examine the products and technical controls your organization uses to identify and mitigate internal threats. Run staff training and awareness sessions, review security incident reports, and perform red team exercises such as phishing tests to identify repeat unintentional insider threats. Then train, warn, and mitigate these individuals by implementing additional security controls on their accounts, systems, privileges, and access. For example, your security team could restrict staff members' ability and opportunity to perform insider threat actions with strict controls and policies. Some examples include:

    - Enforce a policy that macros cannot be enabled or executed on systems.

- Configure all emails to arrive in plaintext with hyperlinks disabled.
- Quarantine all external email attachments by default.
- Disable web browsing, or make it available only through an isolated internet system that is not connected to your organization's intranet.
- Disable USB ports and external media drives on certain systems.

Monitoring intentional insider threats requires both advanced detection techniques and technologies capable of deception and secrecy. Select these based on appropriate organizational threat modeling and risk assessments.

2. *Implement human resource–based anti-*minomushi *policies.* After the previous technical controls and detection techniques have been implemented and tested, address personnel controls. Ensure that human resources maintains records on current employees, previous employees, and candidates that include indicators of *minomushi* profiles. Ask pointed questions during candidate screening, performance reviews, and exit interviews to capture these diagnostics.
3. Human resources should also take special care to prevent the circumstances that create *minomushi* employees. Your human resources team should consider the following organization-wide policies, presented in order of the eight *minomushi* archetypes.

    - Review employee disciplinary protocols to prevent unfair or excessive punishment—real or perceived—of employees. Require that employees and applicants disclose whether they have family members who have worked for your organization. Encourage human resources to gauge whether employees think the disciplinary actions against them are unfair or excessive; then work together to find solutions that will mitigate employee animosity.
    - Regularly distribute employee surveys to gauge morale and identify underutilized talent in lower-ranking employees. Conduct transparent interviews with employees and management to determine whether: an employee is ready for a promotion, has gone unrecognized for recent achievements, or needs to grow a specific skill set; the company has a role to

promote them into or budget to offer them a raise; or certain employees perceive themselves to be better or more valuable than their colleagues—and whether a reality check is necessary. Working with management, consider how to alleviate employee bitterness and how to correct perceptions that the organization is not a meritocracy.

- As part of performance reviews, solicit feedback from colleagues to identify managers whom lower-ranking employees consider most valuable, as well as which employees believe they have not received appropriate recognition. Address these grievances with rewards and/or visibility into the company's leadership decisions.
- Encourage leadership to personally coach smart but socially awkward workers, discretely letting them know how they are perceived, with the goal of helping these employees feel more socially accepted and less isolated.
- Review and eliminate company policies that hold back top talent. These may include noncompete agreements; unfair appropriation of employees' intellectual property; and insufficient performance bonuses or retention incentives. While designed to protect the company, these policies may have the opposite effect.
- Conduct open source profiling of current employees and applicants to determine whether they have publicly expressed strong feelings about or have a conflict of interest in the mission of your organization. If so, reassign those employees to positions where they will feel more alignment between their personal values and the work they do or ease them from the organization.
- Develop character-profiling techniques to look for indicators of that employees and applicants may be susceptible to bribery. Consider reducing system access and privilege levels for these employees, thereby reducing their usefulness to an adversary.

Work closely with employees at high risk for *minomushi* conditions. Give them extra resources, time, and motivation to move past whatever grudges they may hold, seize opportunities for personal growth, and develop self-respect. Minimize or halt organizational actions that reinforce bad memories or continue to punish an employee for past misdeeds.

CASTLE THEORY THOUGHT EXERCISE

Consider the scenario in which you are the ruler of a medieval castle with valuable information, treasure, and people inside. You receive credible threat intelligence that a shinobi plans to recruit someone within your castle to use their trust and access against you. You receive a list of eight different types of people likely to be recruited. It's unclear who specifically is being targeted or what the shinobi's objectives are.

Whom would you first suspect as an insider threat? Why is that person in a vulnerable state, and how could you remediate the situation? How would you detect the recruitment of one of your subjects or catch the recruiter in the act? How might you place guards to prevent insider threat actions? How could you train your subjects to report insider threats without causing everyone to turn on each other? How long should you maintain this insider threat program?

To avoid the political pitfalls of conducting this as a group exercise at your current workplace, consider building and using a list of former employees. If you can perform this exercise discretely with a small group of stakeholders, consider both former and current employees.

Recommended Security Controls and Mitigations

Where relevant, recommendations are presented with applicable security controls from the NIST 800-53 standard. Each should be evaluated with the concept of recruited insider threats in mind. (For more information, see PM-12: Insider Threat Program.)

1. Have the SOC work privately with human resources to correlate information on potential insider threats who display *minomushi* characteristics. The SOC should more closely monitor, audit, and restrict these high-risk individuals. It can also work with human resources to establish insider threat honeypots—for example, files in network shares that say "RESTRICTED DO NOT OPEN"—that identify employees who perform actions consistent with insider threats. [AC-2: Account Management | (13) Disable Accounts for High-Risk Individuals; AU-6: Audit Review, Analysis, and Reporting | (9) Correlation with Information from Nontechnical Sources; SC-26: Honeypots]
2. Use your own account to perform insider threat actions (without red team capabilities) on files and systems you know will not harm

your organization. Actions could include modifying or deleting data, inserting fake data, or stealing data. Document which systems and data your account can access; then use a privileged account such as admin or root to conduct malicious privileged actions. For example, you could create a new admin user with an employee name that does not exist. Ask whether your SOC can discover what data you stole, deleted, or modified within a specific date range to test whether your SOC can properly audit the privileged actions you performed. [AC-6: Leave Privilege | (9) Auditing Use of Privileged Functions; CA-2: Security Assessments | (2) Specialized Assessments]

3. Train your employees to recognize *minomushi* characteristics and insider threat behavior. Enable employees to easily and anonymously report potential *minomushi* conditions with respect to suspected insider threats, similar to how they report phishing scams. Conduct insider threat awareness exercises as part of regular security training. [AT-2: Security Awareness | (2) Insider Threat]

Summary

In this chapter, we reviewed the shinobi technique of recruiting vulnerable people inside a target organization to perform malicious actions. We detailed the eight insider threat candidate archetypes and discussed the various types of insider threat detection and protection programs currently used by organizations. We described a new defensive approach based on information from the shinobi scrolls—one that uses empathy toward the disgruntled employee. The thought exercise in this chapter challenges participants to evaluate not only potential insiders but also their own actions toward coworkers; it encourages them to think about taking a more cooperative approach to potential insider threats.

In the next chapter, we will discuss long-term insiders: employees recruited by an adversary before they joined your organization. And, since long-term insiders intentionally hide any resentment or malice toward the organization, detecting them is even more problematic.