VARONIS
THREAT LABS

THE ATTACKER'S PLAYBOOK

Understand how threats are hacking trust at every stage of the kill chain.

INTRODUCTION:

HACKING TRUST

Trust is a popular attack surface for threat actors.

As organizations embrace AI, cloud platforms, and remote collaboration, attackers are exploiting the same systems designed to empower users by impersonating employees, hijacking sessions, and manipulating workflows. The days of using malware are gone, now that all hackers need is trust. Trust is fragile and easily broken in the digital landscape.

With 86% of breaches involving stolen credentials, the perimeter is no longer the frontline of defense. Identity, behavior, and access have become the battlegrounds, emphasizing that attackers aren't breaking in — they're logging in.

To defend against modern threats, we must understand them. In this playbook, we will explore how threats exploit trust at every stage of the kill chain using real-world examples and highlight specific ways data defenders can fight back.

INITIAL ACCESS = TRUST MANIPULATED

Attackers today are social engineers, reconnaissance experts, and cloud-native operators. They study your environment, mimic your users, and weaponize your workflows. To gain access to your network, threats are using advanced phishing tactics, vishing, deepfakes, and corporate chat abuse as standard tools in their arsenal.

Generative AI enables attackers to be increasingly sophisticated in their methods, turning what used to be laborious recon into trivial time spent. They're not using questionable links or attachments that target one company anymore; they lure users across hundreds of organizations into compromising their credentials, identities, or data. What used to be clumsy, typo-ridden messages are now hyper-personalized, AI-generated emails that bypass traditional filters and exploit human trust.

Bypassing multifactor authentication (MFA), targeting vulnerabilities in internet-facing infrastructure, and remote access vulnerabilities remain common entry points as well, especially when trust in user behavior overrides technical controls.

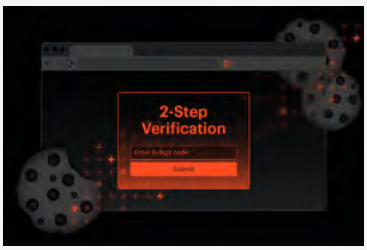
MITIGATION TIP:

Train and test users

Train your employees to identify phishing attempts, validate the identity of the sender, and manage their passwords effectively. Encourage the reporting of suspicious activity and regularly test your cybersecurity team to identify potential risks. Phishing simulations organized by your security team are a great way to see how employees respond to manipulation attempts, in addition to enabling technical controls to protect against remote access mechanisms.

COOKIE-BITE: HOW THREATS CAN BYPASS MFA

In 2025, Varonis Threat Labs uncovered how attackers can use stolen session cookies to impersonate users and bypass MFA entirely — demonstrating how fragile browser trust can be. This method, dubbed Cookie-Bite, exemplifies how trust-based compromise can bypass traditional controls. **Learn more.**



DISCOVERY AND RECON = TRUST-BASED EXPLORATION

Once inside, threat actors explore and observe your environment to determine the best method of attack. Common post-exploitation steps include network scanning, file extension hunting, and AD queries to learn about the computers, users, trusts, and group policies in your environment. Gen AI can accelerate this process by surfacing sensitive data without triggering alerts.

MITIGATION TIP:

Continuous monitoring

Threat detection capabilities that notify you of abnormal activities are the best way to identify an attack while it's in progress. Consider enabling services like **Varonis MDDR,** which provides 24x7x365 network monitoring and behavioral analysis.

PERSISTENCE = TRUST MAINTAINED

Maintaining access is crucial for attackers, with trust being a key element in how they blend in. Threat actors often use Living of the Land Binaries (LOLBINs), Remote Monitoring and Management (RMM) tools, and network tunnels to avoid detection.

Fortunately, network-based detections can help protect your environment. Using firewall, proxy, or DNS data, alerts focused on MFA modifications, admin groups, and other privileged roles often capture threat actors seeking to maintain high-level access.

MITIGATION TIP:

Default deny all

Configure your firewalls/proxies to deny all traffic between your servers and the internet by default, implementing an allow list for required communications. Although this can be time-consuming, this setting severely limits the movements of a threat actor who manages to breach your network, giving your SOC a head start to contain the threat.

PRIVILEGE ESCALATION = TRUST ABUSED

Once threats are comfortable, misusing trust is the next step. They escalate privileges by exploiting misconfigurations and identity gaps, such as Active Directory (AD) exploitation, Kerberoasting, and attacking trusted processes such as LSASS to reset login credentials and modify account privileges. Overly permissive accounts and passwords stored in insecure locations, such as AD descriptions and GPO Scripts on SYSVOL, create easy wins for adversaries.

MITIGATION TIP:

Least privilege enforcement

Adopting a least privilege approach to permissions is the best way to limit the impact threats can have at this stage. You can also use tools like SharpHound to audit Active Directory and Entra before the bad guys do.

WHEN THREATS ARE AUTHORIZED TO ATTACK

In 2025, UNC6040 and **Scattered Spider** bypassed technical defenses by impersonating IT support with the help of vishing tactics and exploited Salesforce's OAuth flow. Victims unknowingly authorized rogue apps, handing over access tokens that allowed attackers to siphon customer data undetected. **Learn more.**

IMPACT & EXFILTRATION = TRUST BETRAYED

Once an attacker has gained knowledge from silently lingering in your environment, it's time to strike. They'll begin to exfiltrate data and impact organizations.

Most attackers use cloud-native platforms like Azure, AWS, and Box to exfiltrate data due to limited coverage from security tools that don't offer visibility into how data moves in these environments. Attackers may also host their own services or use tools like FileZilla and WinSCP to blend into normal traffic. Ransomware as a service (RaaS) groups like **LockBit 3.0** and **BlackCat/ALPHV** can amplify the impact, often turning data theft into public extortion.

MITIGATION TIP:

Maintain deep visibility of data

Data is attackers' main target. If your current security stack can't see how data flows from your environment to cloud platforms, third-party tools, etc., the impact of a breach can be catastrophic. Enable a data security solution that includes cloud-native DLP, with specific capabilities that automatically discover and classify sensitive data at rest, prevent exposure, monitors data activity, and stops data exfiltration.

PHISHING IN PLAIN SIGHT

Forensics experts from Varonis Threat Labs uncovered a novel phishing campaign targeting more than 70 organizations through a lesser-known Microsoft 365 feature, Direct Send. The attackers used the trusted infrastructure to move data stealthily — never triggering outbound alerts. **Learn more.**

AI & IDENTITY = TRUST IN TECHNOLOGY

AI copilots, chatbots, and internal LLMs are increasingly over-permissioned and under-monitored. Attackers and insiders alike can exploit these tools to surface and leak sensitive business data at scale. Identity management gaps, lack of least privilege enforcement, and AI's role in creating data compound the risk.

The answer isn't to disable and avoid AI tools. Employees will still use AI tools for work purposes despite them being blocked or unmonitored, increasing shadow AI use and limiting your security team's visibility into user activity.

Organizations and security teams need to fight malicious AI with AI. They need to be able to visualize AI's sensitive data access, revoke excessive permissions, monitor prompts and enable alerts on suspicious activity, classify AI-generated content properly, and enforce AI guidelines for the enterprise.

MITIGATION TIP:

Deploy AI securely with confidence

Find a security solution that secures AI agents, monitors data flows, and reduces every user's blast radius through automated policy enforcement. Combining AI-related security features with modern identity detection and threat response, classification, and DLP solutions also enhances your ability to improve your security posture, untangle permissions, and detect anomalous activity.

ONE CLICK TO COMPROMISE

EchoLeak, a one-click exploit discovered by Aims Labs in Microsoft 365 Copilot, revealed how attackers could prompt AI copilots to surface sensitive data without ever breaching a perimeter. Trust in AI became the vulnerability, and the result gave threats the ability to silently extract sensitive and proprietary information all from a single email. **Learn more.**

REBUILDING TRUST THROUGH DATA SECURITY

Trust is no longer a passive assumption — it's a dynamic risk surface.

The attacks and methods we've outlined in this playbook aren't driven by zero-days or exotic malware. They're driven by psychology, routine, and misplaced confidence. Threat actors are exploiting the systems normalized workflows, and trusted identities that enterprises rely on. And they're doing it faster than most organizations can adapt.

For security leaders, the challenge is strategic: how do you secure systems built on collaboration, identity, and automation without slowing down the business? For practitioners, the challenge is tactical: how do you detect and respond to threats that look like normal behavior?

To defend against trust-based attacks, the entire organization's mindset must shift from perimeter defense to data-first security. That means automating outcomes, reducing risk, and protecting data. It's no longer about keeping threats out — it's about understanding how they get in, how they blend in, and how they move through environments built on convenience and collaboration.

Organizations that thrive will be the ones that treat trust as a living asset — monitored, measured, and managed with the same rigor as any other critical resource.

YOUR DATA. OUR MISSION.

ALL IN ONE-PLATFORM

Secure your most valuable asset with the industry's most complete data security platform. Varonis is your all-in-one solution to automatically find critical data, remediate exposure, and stop threats.

Platform overview ›

VARONIS INTERCEPTOR

Protect against the sophisticated phishing and social engineering attacks we've outlined in this guide with Varonis Interceptor, our AI-native email security solution with the best detection rates on the planet.

Interceptor overview ›

VARONIS MDDR

Protect your business from material data breaches with 24x7x365 incident response and alert monitoring from Varonis data security experts through our Managed Data Detection and Response service.

MDDR overview ›

Partner with the leader in data security.

Gartner

#1 DSPM vendor
on Gartner Insights

FORRESTER®

Leader in Forrester Wave™:
Data Security Platforms,
Q1 2025

GIGAOM

Leader in GigaOm Radar
for Data Security Platforms
(DSPs)

Meet Varonis Threat Labs

Varonis Threat Labs (VTL) is our team of security researchers, forensics investigators, and data scientists that are among the most elite cybersecurity minds in the world. With decades of military, intelligence, and enterprise experience, this team investigates threat actor groups, misconfigurations, vulnerabilities, and other risks to data daily.

Explore more of Varonis Threat Lab's findings on our blog.

About Varonis

Varonis (Nasdaq: VRNS) is a leader in data security, fighting a different battle than conventional cybersecurity companies. Our cloud-native Data Security Platform continuously discovers and classifies critical data, removes exposures, and detects advanced threats with AI-powered automation.

Thousands of organizations worldwide trust Varonis to defend their data wherever it lives — across SaaS, IaaS, and hybrid cloud environments. Customers use Varonis to automate a wide range of security outcomes, including data security posture management (DSPM), data classification, data access governance (DAG), data detection and response (DDR), data loss prevention (DLP), and insider risk management.