VARONIS
THREAT LABS

THE ATTACKER'S PLAYBOOK

Understand the mindset of a threat actor to strengthen your security posture.

UNDERSTANDING ATTACKER BEHAVIOR

The rise of generative AI and ransomware as a service (RaaS) directly impacts how threat actors infiltrate your networks — **they no longer break in; they log in.**

There are often early indicators when a threat is present in your environment. Still, many organizations struggle to understand the steps attackers take to gain access and where there are vulnerabilities. Identifying how hackers think and their steps can turn your team into formidable defenders and improve your data security posture.

In this guide, we share how an attacker thinks during each stage of the kill chain, why it's crucial to know a threat actor's points of view (POV) to defend against them, and mitigation tips from our research and forensics experts.

FROM A THREAT ACTOR'S POV

Every threat actor is after the same thing — your data. Thinking about a data breach through the enemy's eyes can help your organization respond properly to an attack. Below are some attacker tactics and POVs that cybersecurity leaders should keep in mind.

POV 1 \\ GAINING INITIAL ACCESS

Adversaries need a way in, and manipulating users is a common method they use to gain access to your network. This includes phishing attempts, MFA bypasses, and man-in-the-middle (MITM) attacks.

Most breaches start with a bad actor gaining credentials through one of these techniques, followed by using legitimate corporate applications such as VPN or VDI environments. Ensure you have MFA applied to all remote access vectors of your network to help protect against credential compromise events.

MITIGATION TIP:

Train and test users

Train your employees to identify phishing attempts 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.

POV 2 \\ TAKING A LOOK AROUND

Unlike a typical thief who must act quickly, threat actors seeking your data spend time observing your environment to determine the best method of attack. Locating sensitive files has become even easier for malicious actors with the addition of **gen AI tools,** which can surface and leak critical information to internal users or threats due to over permissions.

Common post-exploitation steps include share scanning, internal port scanning, and AD queries to learn about the computers, users, trusts, and group policies.

MITIGATION TIP:

Continuous monitoring

Threat detection capabilities that notify you of abnormal activities are the best way to stop an attacker from gaining privileged access. Consider enabling services like **Varonis MDDR,** which provides 24x7x365 network monitoring and behavioral analysis.

POV 3 \\ KEEPING IT SIMPLE

Threat actors like to employ the easiest method to remain undetected. One might use an RMM tool to maintain persistent access to a breached environment via network tunnels, using software like SSH, ngrok, cloudflared, or SOCKS proxies.

Fortunately, network-based detections can help defend 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 does manage to breach your network, giving your SOC a head start on containing the threat.

POV 4 \\ GOING AFTER THE ADMIN

Administrative rights can provide malicious actors access to your most confidential information, making it a primary target for attackers.

Gaining domain administrator privileges or equivalent levels of access grants attackers the "keys to the kingdom," enabling them to reach any system within your network and gain access to all credential hashes maintained in Active Directory. Recovering from this level of data breach can be a difficult challenge.

Admin credentials are often overly distributed in Salesforce environments due to time constraints, leading to many internal users with elevated privileges. Providing system-wide access in Salesforce and similar cloud services allows users to see all data, posing a serious threat to your organization.

MITIGATION TIP:

Practice least privilege

Prescribe the exact privileges needed for users and service accounts to achieve their goals without over-provisioning. Organizations often make service accounts domain admins because determining the exact permissions required on a case-by-case basis can be time-consuming.

Instead, provide users with temporarily elevated privileges (just-in-time elevation) as their role necessitates rather than making them "always-on" administrators. This can help mitigate the impact should a user's account be compromised in the future.

POV 5 \\ LOOKS LIKE A JOB FOR RANSOMWARE

Financially motivated threat actors tend to use ransomware tactics to create mass-impact events. With the rising popularity of **RaaS**, companies and organizations of all shapes and sizes should be well-versed in reducing the chances of a ransomware attack.

MITIGATION TIP:

Enable a team of defenders

If you're concerned about ransomware's impact on your environment, don't wait for a breach to occur. Employ a defense, such as Varonis MDDR, that watches your data 24x7x365 and responds to ransomware incidents immediately following an event.

YOUR DATA. OUR MISSION.

This guide was brought to you by our **Varonis Threat Labs** and **Varonis MDDR** teams. Watch our **past live event** discussing the Attacker's Playbook for more insights and contact us if you have any questions.

Partner with the leader in data security.

Gartner

#1 DSPM vendor
on Gartner Insights

FORRESTER®

Leader in Forrester Wave™:
Data Security Platforms,
Q1 2023

GIGAOM

Leader in GigaOm Radar
for Data Security Platforms
(DSPs)

Reduce your risk without taking any.

Our free Data Risk Assessment takes minutes to set up and delivers immediate value. In less than 24 hours, you'll have a risk-based view of the data that matters most and a clear path to automated data security.

Get a demo at www.varonis.com/demo.

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.