jamf

Anatomy of an attack

In today's globally connected world, cybersecurity professionals have their work cut out for them against threat actors. While the latter only needs to exploit one vulnerability or compromise one set of credentials to gain a foothold onto organizational networks, you as the former must get it right every. single. time... or run the risk of a non-compliant device or user credentials potentially opening the door for a data breach.

As Thomas Jefferson said, "knowledge is power." In this case, that power can arm threat actors with insight into the failings of an organization's defenses or it allows cybersecurity professionals to understand the nature of a cyberattack used against them.

To do that, you need to look at each phase of the cyber kill chain and carefully examine the anatomy of such an attack. By doing so, you can shore up risks while fortifying protections.

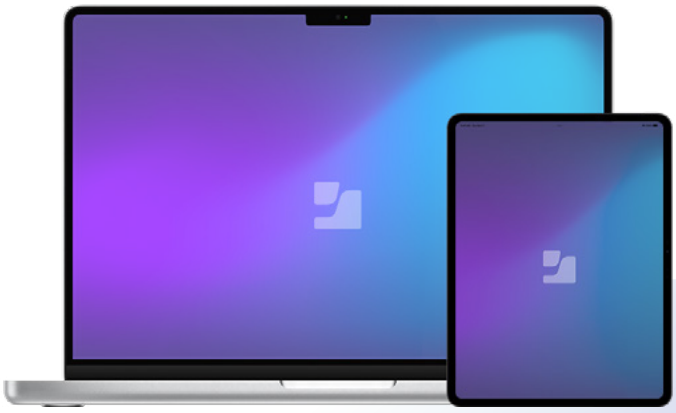
In this technical paper, we:

- Breakdown the cyber kill chain
- Provide a demonstration of how an attack works
- Align key links with critical protections
- Underscore the criticality of closing security gaps

Break it down again

Attacks vary because the threats that bad actors choose to incorporate are based on the target(s) selected and what vulnerabilities they hold. While utilizing similar aspects, the uniqueness of attacks combined with the variables that impact an endpoint's security is enough to make cybersecurity a mix of art and science to deduce.

However, despite the variation of threats that make up an attack, one certainty is the anatomy of an attack or links in the **cyber kill chain**, as developed by Lockheed Martin. Made up of seven phases to achieve their objective(s) spanning from initial preparation to executing malicious tools by analyzing each phase, cybersecurity professionals can identify breakpoints in their armor that threat actors will target and exploit to bypass defenses.



"So those are my schemes, And these are my plans"

– Tears for Fears

Before learning how to read an attacker's roadmap, here are the seven phases of the cyber kill chain:

1. **Reconnaissance**
Research and identify targets both online and offline.

2. **Weaponization**
Use research gathered to develop and/or procure tools used in later stages.

3. **Delivery**
Malicious tools are actively used against targets to gain access.

4. **Exploitation**
Once access has been obtained, vulnerabilities and other security gaps are leveraged to further extend access.

5. **Installation**
Deployment of malicious code establishes a foundation for the success of the campaign.

6. **Command and Control:**
Communication with compromised devices is established ahead of the final phase of the attack.

7. **Actions on Objectives**
With all preparation and foundational work completed, threat actors execute tools that carry out their goals (gather PII, exfiltrate data, execute ransomware, etc.)

It’s showtime!

Let’s take a granular look at each phase of the cyber kill chain. In this section, we will use the Malware-as-a-Service distributed threat targeting macOS known as **Atomic Stealer** (AMOS) for our example of the anatomy of an attack and how it could be carried out in a real-world scenario.

1.

Reconnaissance

In the intelligence-gathering phase, threat actors focus exclusively on researching their target to obtain detailed information about the victim’s infrastructure, network topography, up and downstream service providers. Any detail helps them to create a profile on the organization that’s targeted. It’s important to note that passive and active reconnaissance can occur during this phase.

Active

This can tip off organizations that they are being surveilled by invasive tools that leave digital fingerprints, such as excessive failed login attempts or network fingerprinting.

Passive

This largely relies on open-source reconnaissance to anonymously gather information without giving the target a heads-up. Examples of this are:

- Using social media to target victims in high-value industries, like crypto.
- Using social media to match employees to critical roles within the target organization
- Identifying vendor partnerships to determine services used by the target to carry out business functions
- Social engineering to trick employees into divulging sensitive or confidential information that can be used in to increase the success of the attack

2.

Weaponization

After completing reconnaissance, threat actors organize the intel they’ve gathered and begin to customize tools that will be used in the earlier stages of the attack. For our example, threat actors performed several tasks to weaponize Atomic Stealer. They developed the malware and ad hoc signed the DMG. Going so far as to provide specific installation instructions for users to bypass Apple’s Gatekeeper warnings. A malicious website was created to mimic the real Arc browser website where visitors were directed to download the compromised version of the software.

NOTE: During phases 1-2, security solutions aren’t particularly effective at stopping the cyber kill chain because it’s mostly conjecture until phase three. Think of it this way, unlike Minority Report, at stages 1 and 2, no attacks are occurring. All that exists are thoughts, ideas or hypotheses in a threat actor’s head. Starting with phase three is where cyber crimes begin and we must wait for threat actors to attempt to commit one before they can be stopped.

3.

Delivery

During this phase, threat actors put their research and tactics into action.

STEP 1. Imitation website goes live

STEP 2. It’s delivered via sponsored ads instead of the legitimate Arc Browser site

STEP 3. User downloads and runs the software which compromises the endpoint with the Atomic Stealer malware

Due to the reach of sponsored ads and placement at the top of user searches, targeting individuals on their devices can lead to scores of infected endpoints in a relatively short time. While this particular attack does not launch by visiting the website directly, likely as a means of evading detection. As noted by Jamf Threat Labs, attacks utilizing variants of Atomic Stealer were found to quickly proliferate as threat actors deploy phishing campaigns using email, SMS and social media to reach a larger pool of victims.

Solutions like **Jamf Pro** and **Jamf Protect** work in tandem to secure users against threats. The former utilizes a combination of content filtering to block phishing URLs, even if users click on the link. Endpoint security actively monitors device health and alerts admins of compliance status changes as device management enrollment profiles enforce data security by keeping business data on a separate, encrypted volume from personal data to prevent commingling. Should business data be impacted, admins can automate device sanitization workflows, including wiping sensitive data from impacted devices to prevent disclosure.

4.

Exploitation

Though the payload delivery method may differ, according to Jamf Threat Labs' extensive research, *"Its goal and logic, however, ultimately remain the same."* In other words, the affected user's credentials are still compromised and their sensitive data is exfiltrated.

That is precisely the aim of Atomic Stealer — the theft of user data after tricking users into entering their credentials as part of the automatic updates process is actually an AppleScript call based on the 'osascript' command native to macOS.

It should be noted that while the actions performed in the background by this malware are documented extensively by **Jamf Threat Labs** (and later in the Actions on Objectives section), the detection of variants based on this malicious code, or even those uniquely developed to evolve over time, offers threat actors the opportunity to perform any number of actions without users becoming aware that they may be affected. Such as being spied on by **threats that bypass Apple's Transparency, Consent and Control framework.**

Even if threat actors succeed in compromising a user's credentials during the phishing campaign, Jamf Trusted Access works to stop further attacks along the cyber kill chain by gathering rich telemetry data in real time, informing admins of device health status changes. Furthermore, it triggers the automatic execution of remediation workflows, such as deploying updates to patch vulnerabilities, preventing the exploit phase from carrying forward.

As for the credentials themselves, **Jamf Connect** manages identity and access which permits the disabling of affected accounts until incident response can occur. For faster **incident response and recovery,** integration with Jamf Protect enables **Zero Trust Network Access** (ZTNA) to automatically minimize risk by identifying when affected credentials are being used to compromise other apps/services. It isolates threats to impacted services but prevents lateral movement across your infrastructure while keeping users productive on unaffected services. Finally, ongoing hardware and software checks occur each time a request is made, providing an additional layer of protection that keeps access to business resources by compromised devices and credentials effectively disabled until verification workflows remediate and determine that impacted devices are compliant.

5.

Installation

Threat actors continue running malicious code and deploying malware to establish persistence. This maintains their access to compromised systems as they conduct additional probes to extend their reach through lateral movements throughout the network that compromised devices are connected to, by leveraging custom and native tools, such as command-line utilities and malicious code to create backdoors. As it relates directly to AMOS, since its goal is simply to steal all the user's information in one go without leaving much of a trace on the system, Atomic Stealer takes minimal steps in this stage. For other attacks, typically this phase facilitates current and future operations to be carried out under cover of stealth.

It is critical to defend against this phase by **leveraging visibility and security to ensure compliance** is being upheld by detecting, preventing and remediating known threats. Actively monitoring device health alerts admins to baseline changes in a device's security posture to triage

and kick off incident response workflows. Jamf Protect prevents known malicious code from being run, including quarantining and removing malware threats before they can run. For unknown threats, device logs are forwarded to a third-party SIEM solution to aid **threat-hunting teams** in detecting and removing threats that may lurk hidden within systems, gathering data as threat actors bide their time.

6.

Command and Control (C2)

The aim of Atomic Stealer is firstly, to steal your credentials; secondly, to use pilfered passwords to steal your data. But depending on the further aims of the threat actor, that doesn't mean the ride stops there. As Keychain offers central, secure storage of credentials, scrapping this rich resource often provides attackers the keys to various functions, software and services. This is an attractive prospect for:

- Obtaining greater access to data-rich resources
- Extending attacks through lateral movements
- Making more money by selling and/or extorting victims

Simply put: more data equals increased lucrative opportunities.

Preventing communication with compromised devices is crucial. ZTNA monitors endpoints and blocks connections to malicious services, like C2 servers, effectively cutting attackers off from communicating with compromised devices. Additionally, ZTNA continues to monitor device and credential health for non-compliance, preventing access to protected resources by devices and credentials that have been compromised, and restricting access to non-compliant devices, while working with Jamf Pro to automatically execute workflows to remediate vulnerable and compromised devices.

7.

Actions on Objectives

In this final phase, attackers carry out the full breadth of their plans, be it:

- **Espionage**
- Data exfiltration
- Extortion
- Supply chain attacks
- Cyber terrorism

Or any combination thereof, the result is the fruit of the threat actor's labor. This section is difficult to quantify because just like each organization has unique needs, each attacker will base their actions wholly or partly based on their unique objectives. In the case of Atomic Stealer, the osascript command mentioned previously is used to emulate the look and feel of a legitimate system alert, but instead uses the user's credentials to collect the following forms of confidential data from Apple Keychain:

- Usernames and passwords
- Browser session cookies
- Sensitive user data
- Payment card details
- Crypto wallets
- System metadata

Repair cracks in your armor

Security gaps left by inadequate protections and focusing merely on desktop operating systems leave mobile devices insecure, allowing threat actors to gain a foothold in organizational networks through compromise.

While mobile devices are far from the only risk leading to data breaches, the evolving threat landscape continues to target mobile due to a combination of greater adoption in the workplace and personal devices increasingly being used to access work data. **Jamf Threat Labs research** quantifies this risk with "40% of mobile users running a device with known vulnerabilities." On vulnerable devices, unchecked risk factors allow threat actors to:

- Run malicious code on devices
- Bypass internal security protections
- Gain access to unauthorized business data
- Obtain privacy data without authorization
- Spy on users without their knowledge or consent
- Pivot attacks from the infected device to compromise networks
- Exfiltrate personal and business data, alongside privacy information

Apple is known for blending form and function, style alongside substance. This philosophy extends to a hallmark of their design that is growing in criticality: security and privacy. Several protections are natively included in macOS and iOS-based operating systems to secure devices, users and their data against myriad threats – both at the hardware and software levels.

Threat actors are evolving their attacks with novel threats and emerging malware variants, like the growing Infostealers category. Security based on static signature detection engines alone is challenged to defend against sophisticated threats. Some, like Atomic Stealer, show "completely different development chains rather than one core version that is being updated," according to Dark Reading. Because of this, **sophisticated threats are evading built-in protections** and putting devices, users and data at risk.

"Hackers only need to get it right once; we need to get it right every time."

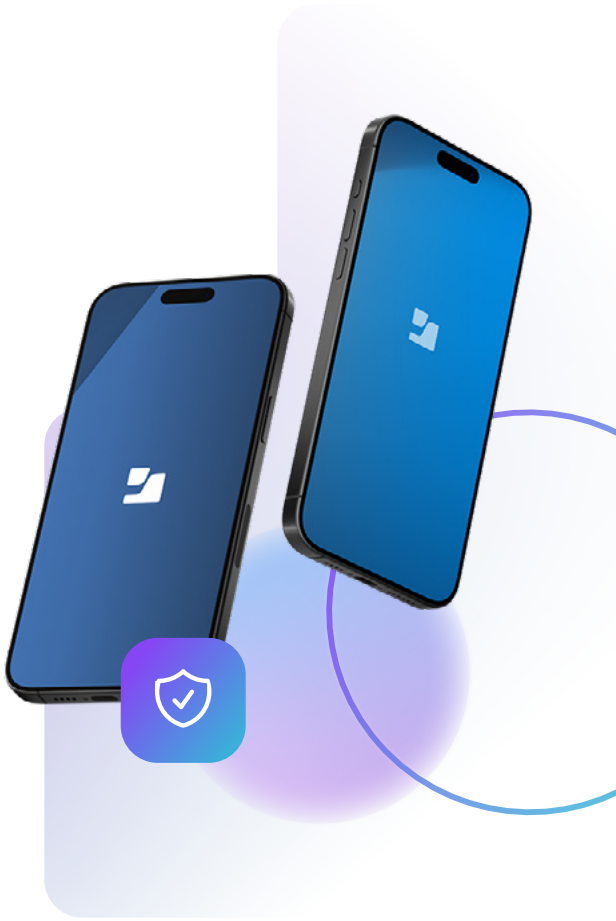
– Chris Triolo, HP

Holistically **integrate management, identity and security as one solution.** Working together – both in-network and on-device – to comprehensively block malicious traffic. Additionally, preventing the exfiltration of business data keeps it safe from attackers. ZTNA drives this workflow by preventing access to protected business services by automatically detecting when credentials have been compromised and disabling them to minimize risk. Because telemetry data is shared securely and holistically, automation executes workflows to mitigate risk vectors until vulnerabilities are remediated. Only after endpoints are verified compliant access to requested resources is approved.

Security plans based on a mature, **defense-in-depth framework** are the best chance organizations have to mitigate risk, prevent known attacks and quickly respond to incidents with automated remediation workflows to maintain endpoint compliance.

Through integrating and layering solutions, organizations defend against sophisticated threats with comprehensive protections to "catch and mitigate" risk through multiple, fail-safe layers. At the same time, these layers of protection extend across the enterprise, providing a baseline of defense for all device and OS types that request access to company resources and data.

According to a recent **Frost Radar: Endpoint Security, 2023 report** on Jamf solutions, Frost & Sullivan noted Jamf as a leader in endpoint security because of the defense-in-depth capabilities of our solutions:



Real-time detection of malicious applications and scripts and recommended user actions.

Consistent vulnerability management, threat prevention and policy control.

Security reporting across all Mac and mobile platforms including macOS, iOS/iPadOS and Android. Additional web threat protection includes these platforms and extends to Windows and Chromebooks.

Expanded configuration and auditing framework to help customers meet complex compliance standards.

Enhanced richness of endpoint telemetry for export to third-party log collection and analytics tools.

Consistent policy enforcement and support for both company-issued and personal devices.

Jamf Trusted Access is the only solution specifically built for Apple devices that combines device management, identity and access, and endpoint security.

Conclusion

As long as threat actors target devices, users and data, security controls will be necessary to minimize risk and prevent threats from leading to more severe data breaches.

The aim of an evergreen security plan should iteratively include:

- Awareness of risk and tolerance levels.
- Implement layers of risk mitigation and threat prevention controls.
- Integrate device management, identity and access, and endpoint security solutions that work in conjunction with one another.
- Converge IT and Security teams, breaking down silos, fostering communication and quickening incident response.
- Leverage automation workflows to remediate threats quickly while minimizing user-introduced errors.
- Align business needs and requirements with standards and frameworks to strengthen security controls and maintain compliance.
- Develop a first responders team to hasten incident response; if a dedicated team is not feasible, establish a partnership with a trusted team of security professionals, like Jamf Threat Labs to aid in threat-hunting for unknown threats.

Partner with **Jamf, a leader in Apple device management and security**. Leverage dedicated **security expertise**, like the Jamf Threat Labs, to close gaps in your security while implementing automated workflows to strengthen your security posture against sophisticated threats while safeguarding sensitive data — for each device accessing protected resources across your infrastructure. Regardless of which device or OS type it is, where it's physically located or what network connection is being used — **Jamf helps your organization succeed with Apple at work**.