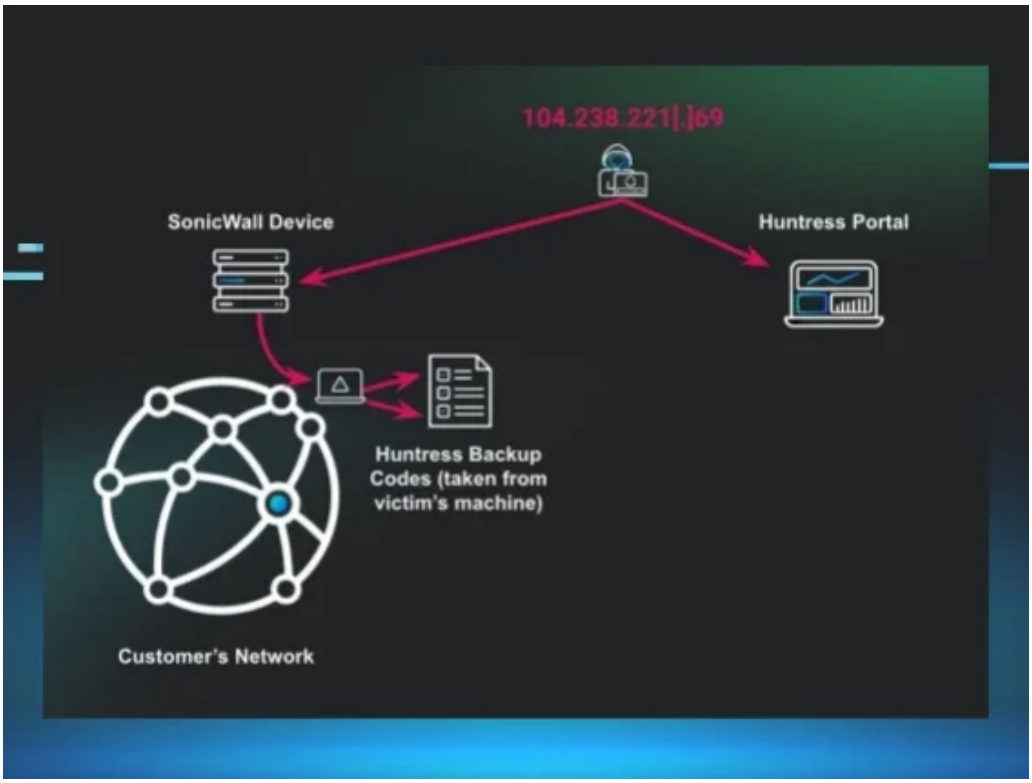
www.huntress.com /blog/dangers-of-storing-unencrypted-passwords

Huntress Threat Advisory: The Dangers of Storing Unencrypted Passwords

Michael Elford ⋮



This is an offshoot of our other blog, "Huntress Threat Advisory: Active Exploitation of SonicWall VPNs," which allowed initial access and was followed by the rapid deployment of Akira ransomware across the victim environment.

This blog outlines an interesting individual case from within that timeframe.

TL;DR: The threat actor entered through the organization's SonicWall device. When searching through the host, the threat actor found a plaintext file on the user's desktop that contained the client's Huntress recovery codes. The threat actor then used these codes to enter the client's Huntress portal and began remediating reports and uninstalling hosts isolated by Huntress.

Key takeaway: Avoid storing recovery codes or credentials in easily accessible plaintext files. Doing so significantly increases the risk of credential compromise, allowing threat actors to pivot to other platforms within the organization. Not all services have safeguards in place to mitigate the impact of compromised accounts, potentially exposing the organization to further harm.

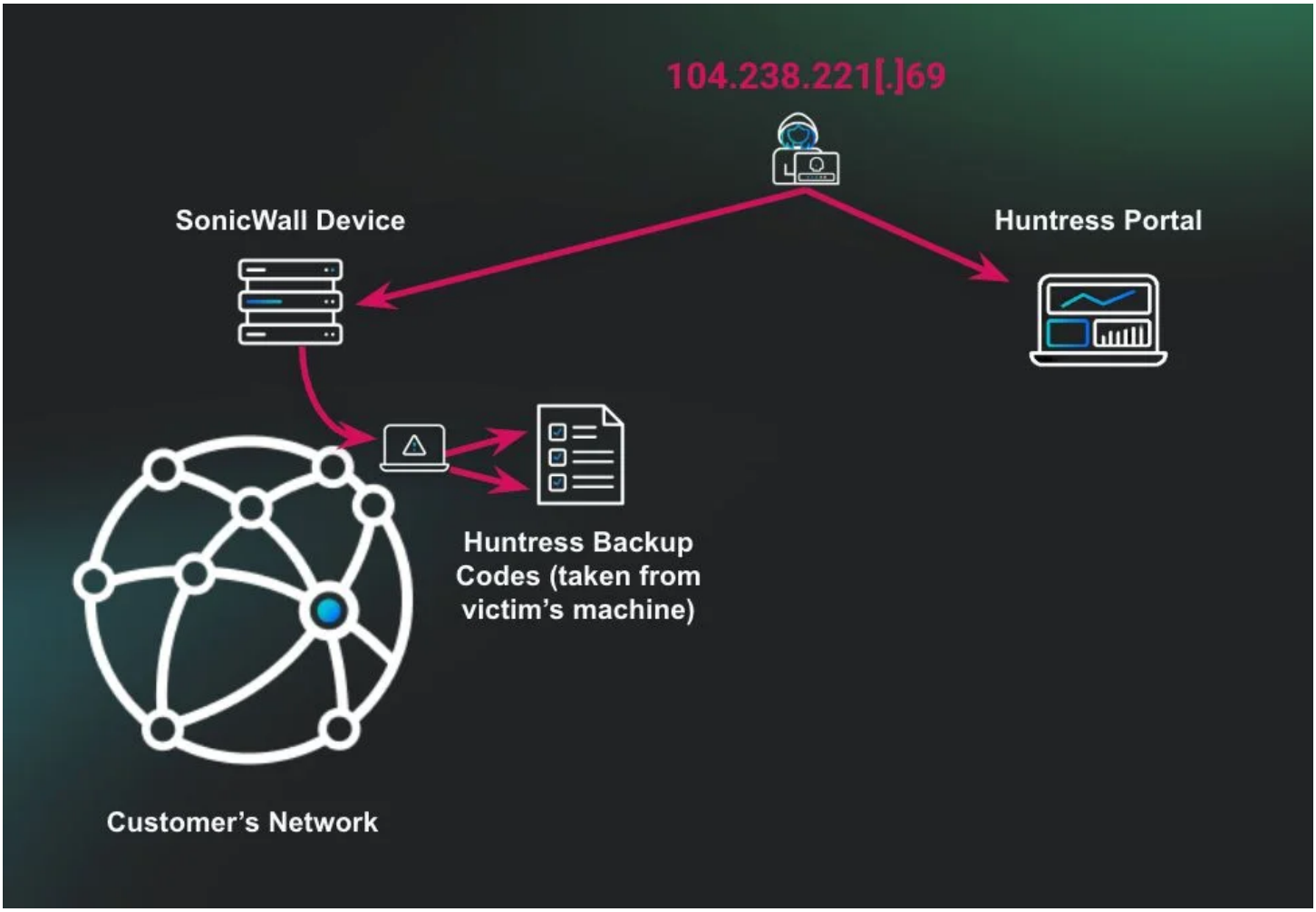


Figure 1: Path of the observed attack

What happened?

The Huntress APAC region's Security Operations Center (SOC) detected multiple administrative users executing commands to delete shadow copies across multiple hosts within an organization. Upon identifying this suspicious activity, analysts initiated a mass isolation response to ensure the threat was contained and to prevent further compromise.

The running process of the Akira ransomware binary w.exe from the user's desktop allowed the workstation to be encrypted. However, the deployment of mass isolation for containment hindered the entire environment from being encrypted.

Triaging SOC analyst Michael confirmed through event log analysis that the affected user accounts were accessed from internal IP addresses in the 192.168.x.x range. These IPs didn't have a Huntress agent installed, likely because they were assigned via DHCP to systems controlled by the Akira threat actors following their compromise of the organization's SonicWall VPN.

This technique is commonly used by threat actors to bypass endpoint detection and response (EDR) solutions. By gaining access through a corporate VPN, threat actors blend in with legitimate internal network traffic, often appearing as trusted users from sanctioned IP ranges.

Since EDR agents are typically deployed only on known managed endpoints, any rogue systems introduced via VPN that lack the agent remain invisible to the EDR. Additionally, activity originating from a VPN-assigned IP can appear as if it's coming from a valid internal source, hindering anomaly-based detections and allowing threat actors to move laterally without immediately raising red flags.

At this stage, the Huntress SOC issued a formal incident report to the organization, outlining the suspicious activity observed and identifying the SonicWall VPN compromise as the likely root cause of the intrusion. The report also provided justification for the immediate mass isolation response. Its purpose was to inform the organization of the threat and guide them through the initial phases of incident response and containment.

Following the report, SOC analysts collaborated with the Threat Hunting & Response team to conduct a deeper analysis of the activity and extent of the compromise. Their objective was to provide the partner with comprehensive context and actionable intelligence regarding the active threat within their environment.

Certificate export and abuse?

While investigating the Domain Controller (DC), analysts observed that a compromised user executed commands to enumerate and export certificates from the local certificate store. Specifically, the attacker accessed the My (Personal) certificate store using the following command:

certutil -store My

This command will list certificates stored under the current user or the machine's personal certificate store. These certificates may potentially contain sensitive keys used for authentication, encryption, or signing.

Shortly after, the attacker exported a certificate identified by its thumbprint (1d967729be08ef8c4bf86874c9542b4e) to both C:\temp\cert.pfx and C:\cert.pfx using:

certutil -exportPFX 1d967729be08ef8c4bf86874c9542b4e C:\temp\cert.pfx

certutil -exportPFX 1d967729be08ef8c4bf86874c9542b4e C:\cert.pfx

Note: Exporting a certificate in PFX format includes both the public and private keys. If the certificate is used for user or device authentication (e.g., VPN or RDP with certificate-based auth), its compromise could allow

threat actors to impersonate legitimate users or machines. This is a common post-exploitation tactic that enables credential theft and lateral movement, especially in environments leveraging certificate-based authentication.

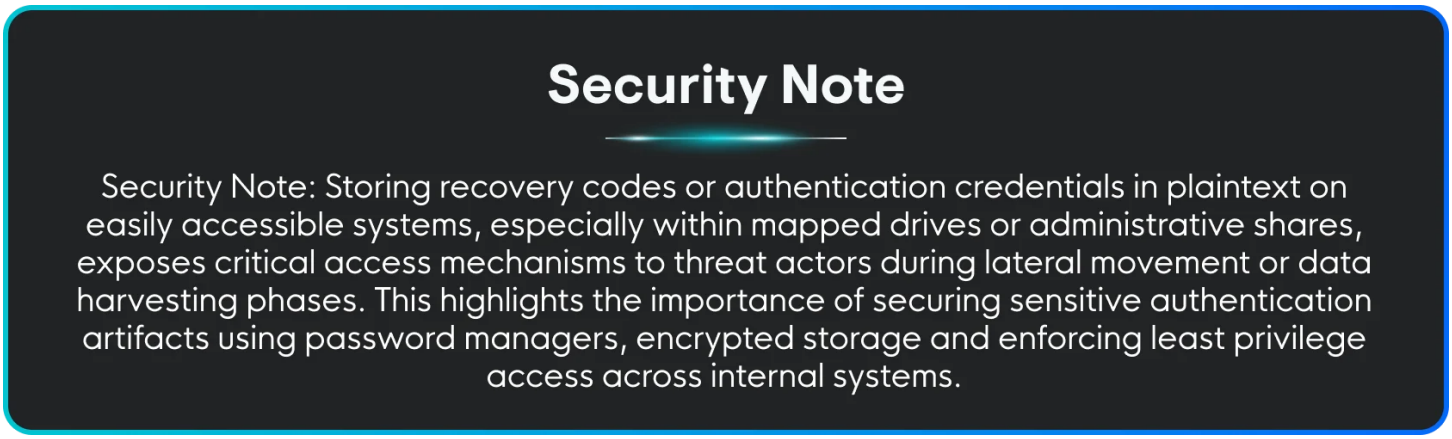
This activity is a strong indicator of a threat actor preparing for persistent access or further privilege escalation. However, we were unable to identify the root cause of this activity during the incident.

Huntress recovery code plaintext

Analysts observed the threat actor actively enumerating administrative shares from the DC, likely in search of sensitive data for exfiltration. During this activity, the actor accessed a plaintext file containing Huntress recovery codes located on an internal security engineer's desktop.

"C:\windows\system32\NOTEPAD.EXE" \\192.168.1.51\c$\Users\
<redacted>\Desktop\Huntress_recovery_codes-<redacted>.txt

These recovery codes serve as a backup method for bypassing multi-factor authentication (MFA) and regaining account access. If compromised, they effectively allow an attacker to circumvent MFA entirely, impersonate the legitimate user, and gain full access to the Huntress console, significantly increasing the risk of further compromise or tampering with detection and response capabilities.



Suspicion of foul play

While triaging the environment and collaborating with SOC Support, analysts noticed unusual activity tied to a security engineer account that had begun resolving active incident reports via the Huntress portal.

Sent	Service	Status	Severity	Entity	Platform	Remediations	Resolved
2025-08-01 04:56:27 UTC		Resolved	Critical				2025-08-01 05:02:11 UTC
2025-08-01 04:53:42 UTC		Resolved	Critical				2025-08-01 05:12:53 UTC
2025-08-01 04:51:55 UTC		Resolved	Critical				2025-08-01 05:12:53 UTC
2025-08-01 04:49:41 UTC		Resolved	Critical				2025-08-01 05:12:53 UTC

Figure 2: Immediate remediation of incident reports by a security engineer account

Given the context of the ongoing compromise, this behavior appeared anomalous and prompted immediate outreach to the partner.

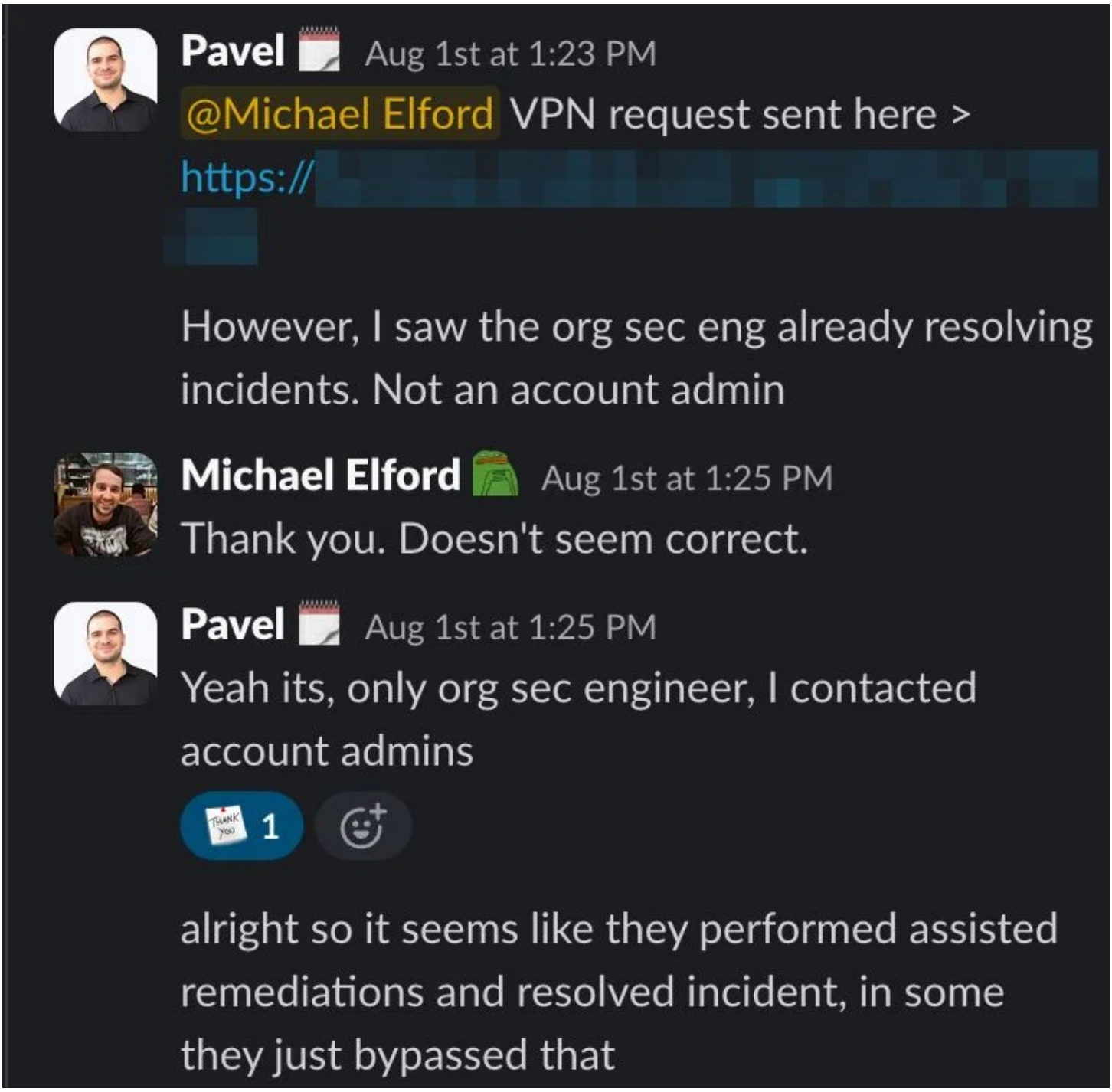


Figure 3: Partner outreach and initial concern raised

SOC analysts quickly escalated their concerns to internal Huntress Support, flagging the suspicious remediations and correlating them with prior findings.

Shortly after the outreach, Huntress Support received confirmation from the partner: the activity attributed to the security engineer account was not performed by their personnel. This revelation confirmed the threat actor had leveraged compromised credentials and recovery codes to access the Huntress portal.

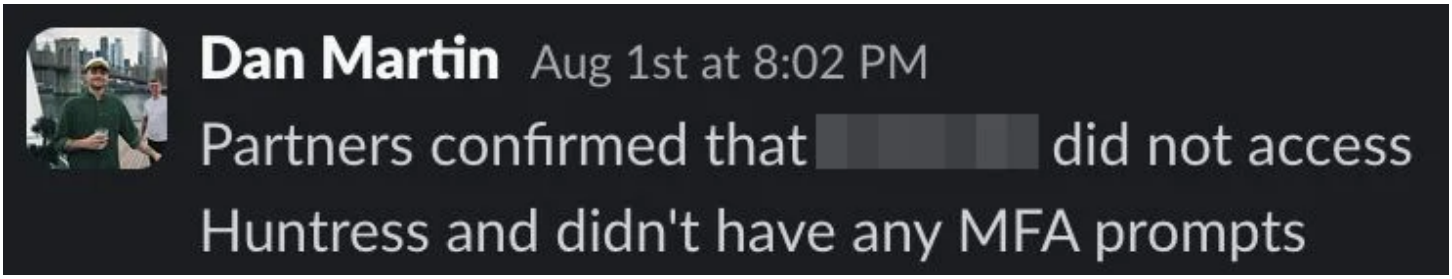


Figure 4: Confirmation of foul play

With this confirmed knowledge, the Huntress team reviewed portal activity. This analysis revealed that a known malicious IP address, 104.238.221[.]69, previously associated with other SonicWall-related compromises, had successfully accessed the Huntress portal using the compromised recovery codes.

```
level       INFO
location    [redacted]
network {
  client {
    geoip {
      as {
        domain    reliablesite.net
        name      ReliableSite.Net LLC
        number    AS23470
        route     104.238.221.0/24
        type      hosting
      }
      city {
        name    Los Angeles
      }
      continent {
        code    NA
        name    North America
      }
      country {
        iso_code    US
        name        United States
      }
      ipAddress    104.238.221.69
      location {
        latitude     34.0614
        longitude    -118.2385
      }
      subdivision {
        iso_code    US-CA
        name        California
      }
      timezone    America/Los_Angeles
```

Figure 5: Huntress portal logon for the security engineer's account

This activity led to the threat actor manually closing active incident reports to suppress visibility and hinder the partner's response. They tasked the de-isolation and the removal of Huntress agents from compromised systems.

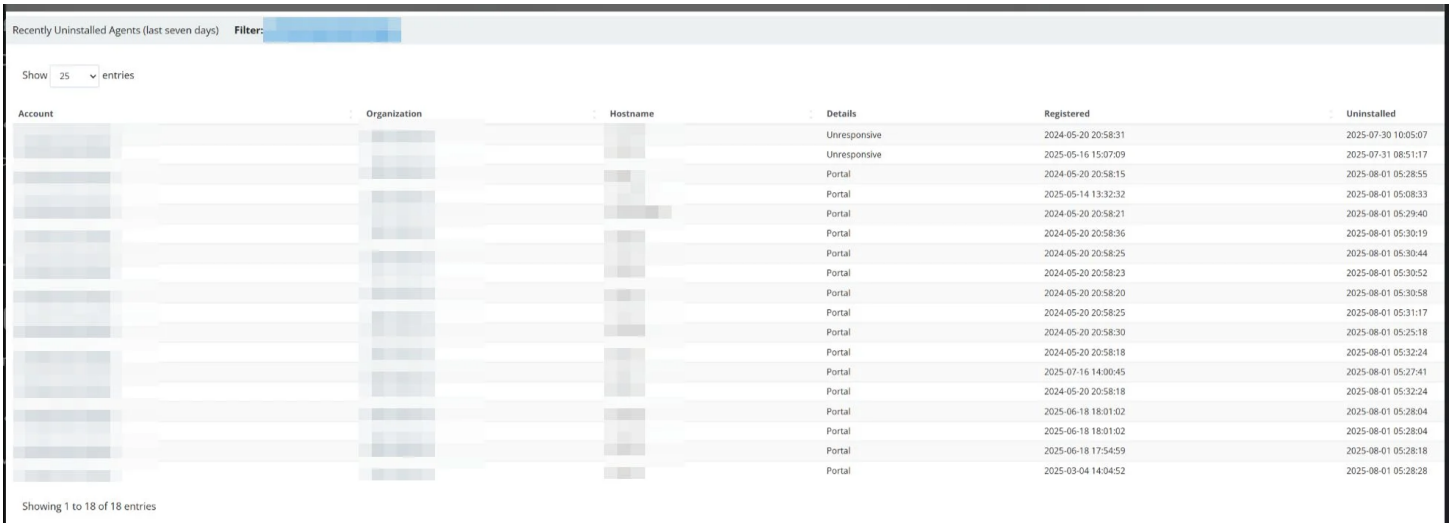


Figure 6: Recently Uninstalled Agents (last seven days) at the time of the incident

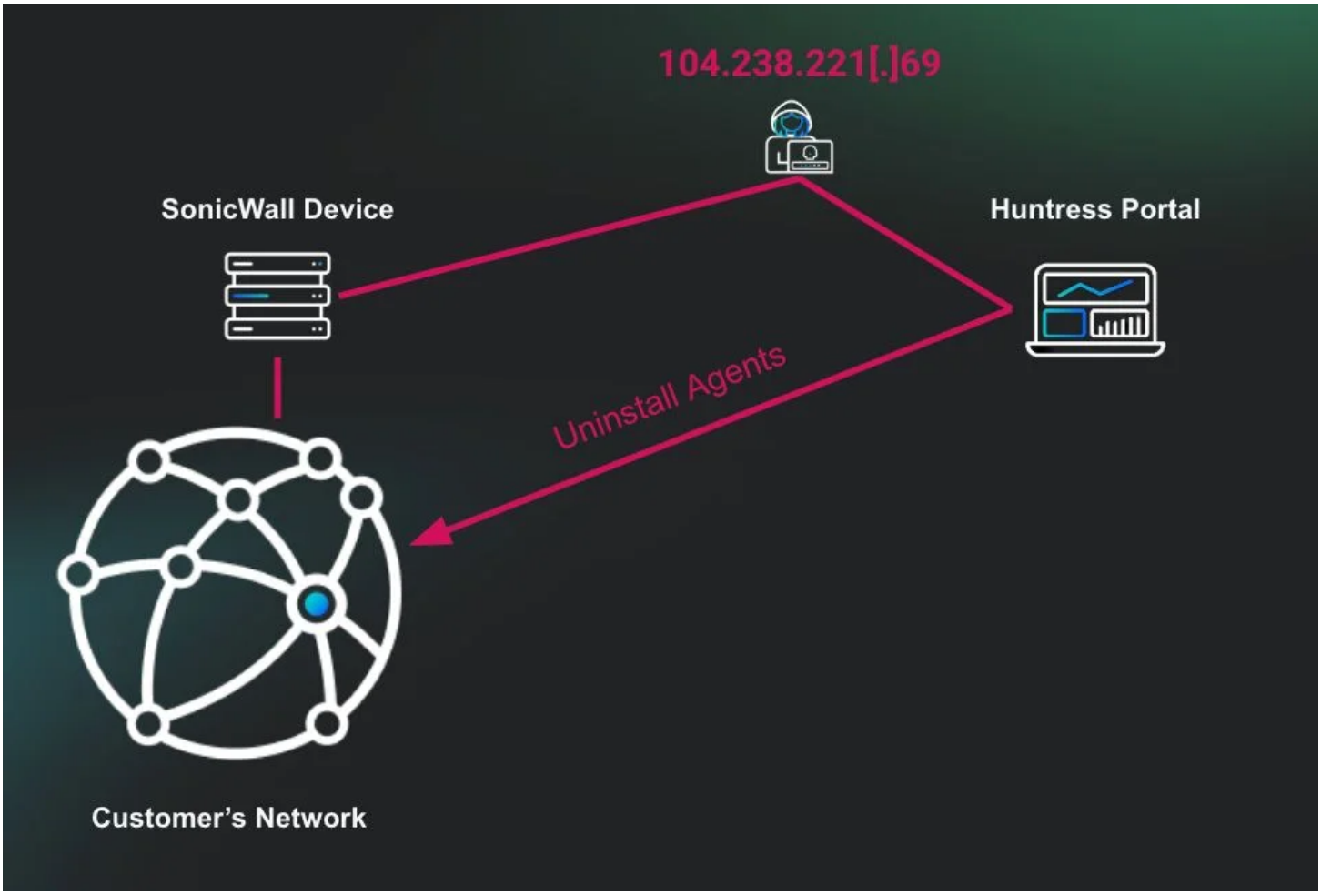


Figure 7: The path of uninstallation of the agents through the portal

This sequence of events underscores the importance of properly securing all forms of authentication mechanisms, particularly **recovery codes**, which are often overlooked as "backup" credentials. In many systems, recovery codes are designed to bypass MFA in situations where users lose access to their primary authentication device (e.g., a phone or hardware token). However, when improperly stored, these codes become a **single point of failure** and grant full access with no secondary challenge.

In this incident, the attacker's ability to enumerate and access recovery codes in plaintext allowed them to:

- **Bypass MFA completely**
- **Impersonate a privileged user**
- **Access the Huntress portal undetected**
- **Suppress incident visibility by closing alerts**
- **Attempt to remove endpoint protections (EDR)**

The dangers of credentials stored in plaintext

Storing credentials and recovery codes in plaintext and in an easily accessible location poses significant security risks (ones that Huntress has seen time and again). Once obtained, these credentials give a threat actor the ability to compromise hosts within the network and access third-party applications and critical security platforms. This level of access can be weaponized to disable defenses, manipulate detection tools, and execute further malicious actions.

In this incident, the attacker used exposed Huntress recovery codes to log into the Huntress portal, close active alerts, and initiate the uninstallation of Huntress EDR agents, effectively attempting to blind the organization's defenses and leave it vulnerable to follow-on attacks.

It's important to mitigate these risks. Organizations should treat recovery codes with the same sensitivity as privileged account passwords. Here are some recommended practices for securing recovery codes and credentials.

- **Avoid plaintext storage:** Don't save recovery codes in unprotected text files, shared drives, or unsecured folders.
- **Use a password manager:** Store recovery codes and credentials in an encrypted password manager with a strong passphrase (and without autofill).
- **Encrypt offline storage:** If you're unable to use digital password managers, store codes in an encrypted, password-protected file on an encrypted USB drive or hard disk.
- **Rotate and monitor:** Periodically regenerate recovery codes if available and monitor login access for unusual logins.

Recovery codes should not be a secondary concern; they are a direct path to bypassing MFA and gaining access.

IOCs

Item	Description
w.exe **SHA256** 6f1192ea8d20d8e94f2b140440bdfc74d95987be7b3ae2098c692fdea42c4a69	Ransomware executable
104.238.221[.]69	Attacker IP entered the Huntress platform
cert.pfx	Certificate Export