White Paper

Compromise Assessments:
For the remote workforce

Make a Plan

Many information technology and security professionals are starting to adjust to the “new normal” of administering a remote workforce and subsequently monitoring for malicious activity of the increased attack surface.

Organizations, large and small, are prioritizing the security of their remote workforce and infrastructure. Compromise assessments are regularly conducted during major business events (e.g. mergers, acquisitions, audits), but are also an important security tool during times like these, where the IT and security teams are overworked, underequipped, or in need of assistance with getting a handle on the increased attack surface ie work-from-home employees.

The threat hunting and configuration guidance below is relevant to a variety of potential network environments depending on size and complexity. We have provided compromise assessment best practices, and guidance on the integration of intelligence feeds to enrich ongoing threat hunting for enhanced security differentiation.

Compromise Assessments and Threat Hunting

When working with a small security team or a hired partner such as a Managed Security Service Provider (MSSP), most actionable anomalies can be drawn back to an event log or a signature-based alert. These alerts come from endpoint protection products, detection and response tools, or Network Security Monitoring (NSM) tools that review activity and compare them to a set of signatures or threat intelligence feeds.

However, when the workforce is remote, gaps in monitoring can present themselves to information security teams and several variables need to be considered. In any of the below scenarios, organizations should standardize a baseline security stack (e.g. AV, DLP, OS hardening, application whitelisting, etc.) to be implemented amongst all corporate assets to ensure consistent visibility of the threat activity landscape throughout the environment.

Scenario 1: Remote workforce without a centralized office

When managing the security stack for a fully remote workforce, there may not be a VPN solution that provides a centralized point to monitor data flow. Deploying a network security monitoring tool may not be a viable solution given there isn't anywhere to physically place the device. The most valuable tool in this environment is the Endpoint Detection and Response (EDR) tool.

The right EDR agent can be deployed to various operating systems, centralize activities and alerts, and enrich the dataset with premium threat intelligence repositories. This level of data provides the analyst a clear view of threat activity across a complex and difficult environment.

Scenario 2: Remote workforce with a centralized office and no requirement to use VPN

Similar to the scenario above, if there is no requirement for the remote workforce to use a VPN, an EDR solution for endpoints is champion of this security stack. While some network-level logs can be collected by EDR agents on endpoints, appropriate network monitoring tools should be installed for better monitoring of the office network.

Organizations should set up a network security monitoring device on the ingress/egress point at the office using a port mirror (e.g. SPAN) or network TAP. While workers during this pandemic may not be in the office as much as they previously were, having any networked resources in the office such as file shares accessible via VPN increases the need to implement an NSM solution in the event someone accesses the resource(s). Additionally, ingesting logs from public facing remote access services, such as the VPN server, into a SIEM would arm the security team with the capability of monitoring authorized and unauthorized attempts to access corporate systems among other activities.

Scenario 3: Remote workforce with a centralized office and no requirement to use VPN

Requiring remote users to authenticate to a VPN to access corporate resources can force network traffic to traverse the VPN server before going out through the office router. By forcing traffic through a central VPN, the organization can monitor network traffic and determine which users access which resources. The security team can then collect logs and alerts from the VPN, NSM, and EDR to correlate user actions and identify indicators of compromise that might exist. The compilation of these datasets can provide the analyst with a holistic view of employee activity.

A Comment on Hybrid Environments

In the cases where an organization maintains both cloud and on-premise resources, it can be difficult to gain the optics necessary to successfully monitor cloud instances. One way Nisos responds to this dilemma is by leveraging the existing technologies within the cloud platform. For example, AWS logging capabilities allow Nisos analysts to review CloudTrail and CloudWatch logs in tandem. By setting up AWS Traffic Mirroring, Nisos analysts collect packet-level network traffic coming to and from the cloud instances. This allows the ingestion of data flow into our NSM tool as if it was collecting it from the router in a corporate office.

The Nisos Way - Moving Beyond Signature-based Detection

Our analysts have years of proven experience deploying and employing monitoring solutions across a variety of networked environments. Not only does our team monitor, research and report activity surrounding the aforementioned actionable alerts, but we go beyond the signature-based anomalies. Our team is looking for the needle in the haystack for which signatures have not yet been created.

Signature-based detection will identify known threats; however, adversaries go to great lengths to defeat security tools and signaturing. Seasoned actors use command and control (C2) channels and exfiltration methods that blend in with an organization's network security baseline. Identifying these sophisticated adversaries is where automated security tools fall short and Nisos excels.

With a fully (or mostly) remote workforce, organizations are dealing with a significantly increased attack surface. Intelligence can be a significant value-add to rapidly identify remote users infected with malware and reduce the risk of an attacker pivoting to the corporate environment. Our external sources provide an unmatched level of visibility outside the perimeter of a corporate or home IT network, allowing us to see suspicious activity from all angles. Nisos can identify malware-infected employees prior to the attacker leveraging a VPN to spread to the internal corporate IT space.

In Conclusion

Full scope visibility is key to determining if the environment has been breached. It is not uncommon for overwhelmed teams to notice they are not fully prepared to take on this level of diligence, especially considering the recent shift in posture to a remote workforce.

For additional information, visit www.nisos.com or contact info@nisos.com