ARISTA

Case Study

Serverless C2 in the Cloud

Industry: Financial Services

Attacker Objective

Live off the land to infiltrate the network

Background

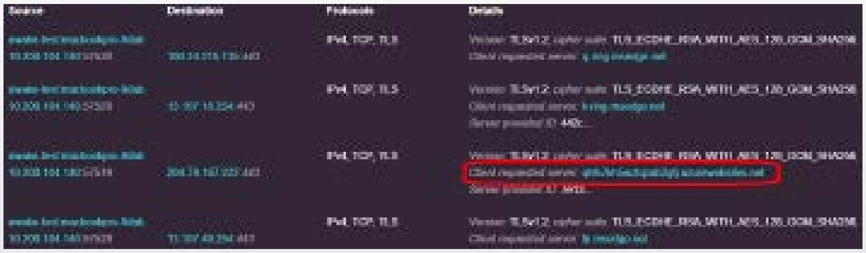
During an engagement with a customer in the financial services industry, Arista NDR discovered a new exploitation technique–serverless command and control (C2) running in the enterprise cloud.

The malware on the customer's network persisted as a Microsoft Office add-in, making it difficult to detect on both the network and the endpoint, as it ran only when certain Office applications were started. These add-ins then downloaded and ran other executables without user knowledge leveraging normal user-level permissions.

Another complicated aspect of the kill chain, in this case, was that the C2 server used Transport Layer Security (TLS) encryption for the communication channel. This allowed the attackers to conceal their actions and fly under the radar of traditional network security solutions. Additionally, the C2 server was serverless code in the Azure cloud, so all that was visible on the network was an encrypted tunnel to a subdomain of azurewebsites[.]net.

Why Arista NDR?

With the ability to identify complex attacker tactics, techniques, and procedures (TTPs) like these, Arista NDR not only caught the serverless C2 but also detected rouge Microsoft Office add-ins used for persistence.



Source	Destination	Protocols	Details
[illegible]	[illegible]	IPv4, TCP, TLS	Version: TLSv1.2, cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 Client requested server: [illegible]
[illegible]	[illegible]	IPv4, TCP, TLS	Version: TLSv1.2, cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 Client requested server: [illegible] Server provided ID: [illegible]
[illegible]	[illegible]	IPv4, TCP, TLS	Version: TLSv1.2, cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 Client requested server: [illegible].azurewebsites.net Server provided ID: [illegible]
[illegible]	[illegible]	IPv4, TCP, TLS	Version: TLSv1.2, cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 Client requested server: [illegible]

Fig 1: Serverless C2 TTP detected using Arista NDR

Arista NDR detected this threat by:

- Identifying outlier connections during the Microsoft Office startup process.
- Using encrypted traffic analysis to identify command and control to a seemingly good domain.
- Correlating multiple threat behaviors to determine the full scope of the attack.

Arista NDR detected this threat because of its built-in knowledge of how applications on the network use sessions and protocols over time. Arista NDR was able to identify connections embedded in the startup-up application fingerprint for Microsoft Word, then isolate outliers from this fingerprint using data science. Finally, using its encrypted traffic analysis and adversarial modeling features, the platform identified the compromised devices on the network.