Serverless C2 in the Cloud

Awake discovered a new exploitation technique, serverless command and control (C2) running in the cloud, during an engagement with a customer in the financial services industry.

The malware on the customer's network persisted as a Microsoft Office add-in. This complicated detection on both the network and the endpoint and ran only when certain Office applications were started, making it more difficult to detect on the endpoint. 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 disguise their actions and fly under the radar of traditional network security solutions. Additionally, the C2 server was actually serverless code in the Azure cloud, so all that was seen on the network was an encrypted tunnel to a subdomain of azurewebsites[.]net.

Awake detected this threat because of built-in knowledge of how applications on the network utilize sessions and protocols over time. In this case, Awake was able to identify connections embedded in the startup-up application fingerprint for Microsoft Word, then isolated outliers from this fingerprint using data science. Finally, the compromised devices were identified based on encrypted traffic analysis and adversarial models triggered in the Awake Security Platform.

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

Source	Destination	Protocols	Details
awake-test:macbookpro-9dab 10.200.104.140:57530	100.24.215.135:443	IPv4, TCP, TLS	Version: TLSv1.2, cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, Client requested server: q-ring.msedge.net
awake-test:macbookpro-9dab 10.200.104.140:57529	13.107.18.254:443	IPv4, TCP, TLS	Version: TLSv1.2, cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, Client requested server: k-ring.msedge.net Server provided ID: 442c...
awake-test:macbookpro-9dab 10.200.104.140:57519	204.79.197.222:443	IPv4, TCP, TLS	Version: TLSv1.2, cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, Client requested server: qhfs7kh5wztqzab2gtj.azurewebsites.net Server provided ID: 7e13...
awake-test:macbookpro-9dab 10.200.104.140:57528	13.107.49.254:443	IPv4, TCP, TLS	Version: TLSv1.2, cipher suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, Client requested server: fp.msedge.net

Microsoft Word starting up, with the malicious add-in present. It downloads and executes the second stage payload from an azurewebsites[.]net function

Industry
Financial Services

Attacker Objective
Live off the land to infiltrate the network

Awake detected this threat by:

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

For additional information about Awake please visit awakesecurity.com

AWAKE