BirdyClient malware leverages Microsoft Graph API for C&C communication

Archived: 2026-04-05 20:42:50 UTC

An increasing number of threats have begun to leverage the Microsoft Graph API, usually to facilitate communications with command-and-control (C&C) infrastructure hosted on Microsoft cloud services. The technique was most recently used in an attack against an organization in Ukraine, where a previously undocumented piece of malware called BirdyClient used the Graph API to leverage Microsoft OneDrive for C&C purposes.

Read more in our blog: **Graph: Growing number of threats leveraging Microsoft API**

Symantec protects you from this threat, identified by the following:

Adaptive-based

- ACM.Ps-Rd32!g1
- ACM.Untrst-RunSys!g1

Behavior-based

- SONAR.TCP!gen6

Carbon Black-based

- Associated malicious indicators are blocked and detected by existing policies within VMware Carbon Black products. The recommended policy at a minimum is to block all types of malwares from executing (Known, Suspect, and PUP) as well as delay execution for cloud scan to get maximum benefit from VMware Carbon Black Cloud reputation service.

File-based

- Backdoor.Graphican
- Backdoor.Graphon
- Trojan Horse
- Trojan.BirdyClient
- Trojan.Gen.2
- Trojan.Gen.9
- Trojan.Gen.MBT
- WS.Malware.2

Machine Learning-based

- Heur.AdvML.A!300

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C
