How CrowdStrike Stops Recent Cozy Bear Phishing Attack

crowdstrike.com/blog/how-crowdstrike-protects-against-recent-cozy-bear-phishing-campaign/

June 10, 2021

CrowdStrike Falcon Protects Customers from Recent COZY BEAR Sophisticated Phishing Campaign

June 10, 2021

Farid Hendi and Liviu Arsene From The Front Lines

A recent sophisticated phishing campaign that delivers advanced malware is targeting diplomatic and sensitive organizations and think tanks around the world. This activity cluster, tracked by CrowdStrike as DiplomaticOrbiter, has been observed using a delivery chain involving lure documents and a sophisticated loading mechanism for payloads.

Based on the targeting profile, CrowdStrike Intelligence currently attributes this recent activity to COZY BEAR, an advanced threat actor acting on behalf of the Foreign Intelligence Service of the Russian Federation, also known as SVR. The malware observed

as part of this activity is also referred to as EnvyScout, BoomBox, NativeZone and VaporRage by the security industry.

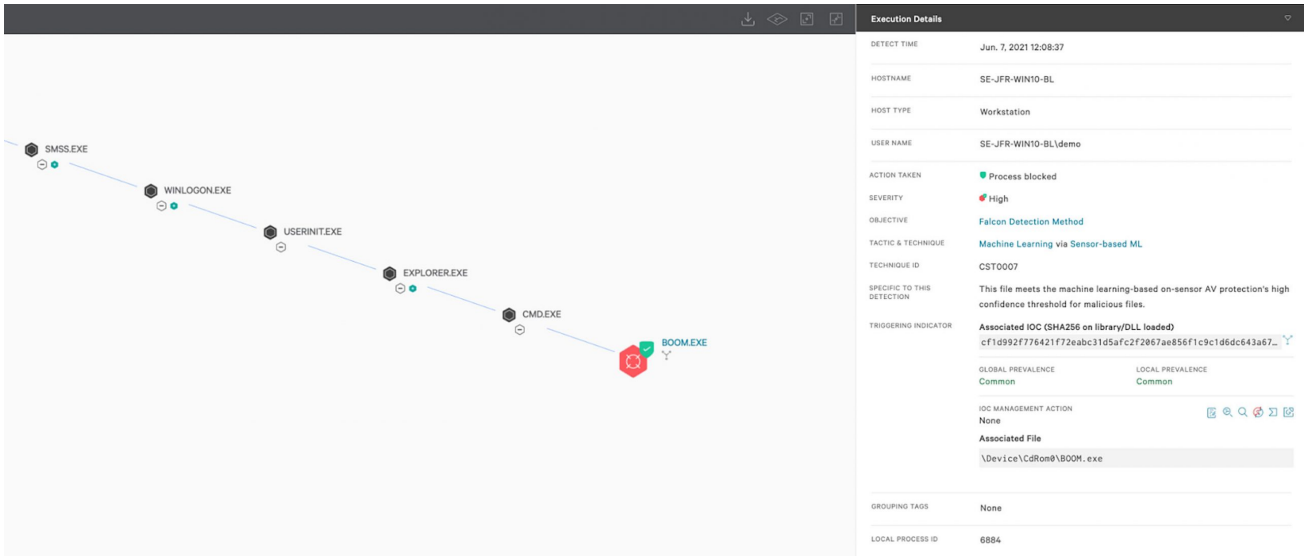
According to CrowdStrike's analysis, the DiplomaticOrbiter activity cluster has been in operation since at least October 2020 and is currently conducting active campaigns focused on sensitive government organizations and Western think tanks. The campaign uses a distinctive delivery chain, employing spear-phishing emails, HTML lure documents and a multistep loading chain for Cobalt Strike Beacon.

This adversary's capabilities are considered to be designed around flexibility and stealth, enabling them to communicate via legitimate channels, conduct advanced victim environment assessment and deploy additional payloads while covering forensic artifacts used in investigations. We continuously track the tactics, techniques and procedures (TTPs) associated with this activity cluster, constantly updating the CrowdStrike Falcon® platform to protect customers against similar attacks.

How Does CrowdStrike Falcon Protect Customers?

The Falcon platform can identify the current tooling associated with the campaign — it continuously monitors TTPs associated with over 160 identified threat actors and numerous unnamed groups, and derives and incorporates intelligence to protect customers and their critical systems.

As soon as the Falcon sensor identifies processes associated with the currently employed tooling, it stops an attack before it can expand. The example below demonstrates how Falcon detects the COZY BEAR run key and interrupts the attack chain by blocking its execution.



(Click to enlarge)

This video also demonstrates how CrowdStrike Falcon can successfully detect and block the tools associated with the recent COZY BEAR campaign.

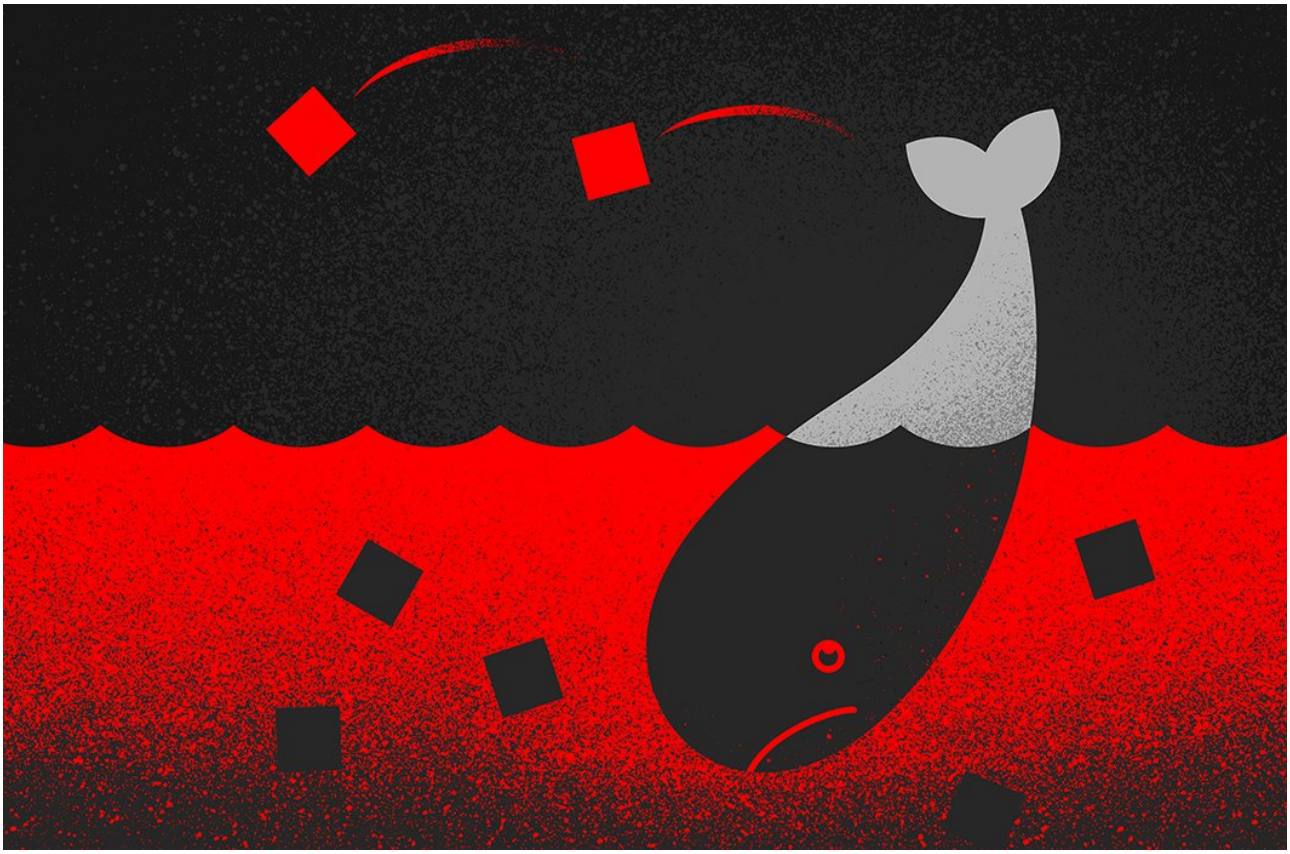
Through a single lightweight agent, Falcon integrates machine learning and behavioral detection to detect and block malware, tools and activities operated by sophisticated adversaries. Coupled with the power and scale of the cloud to analyze large-scale threat telemetry and derive actionable intelligence, the Falcon platform can immediately detect and block behavior and tactics associated with sophisticated adversaries.

Protecting our customers from sophisticated adversaries is something the Falcon platform does every day. The Falcon platform accurately identifies and blocks sophisticated adversaries and threats. Coupled with CrowdStrike's "1-10-60 rule" — detect a threat within the first minute of intrusion, investigate and understand the threat within the first 10 minutes, and contain and eradicate the threat within 60 minutes — as a benchmark for swiftly defeating adversaries, Falcon helps organizations secure their operations and stop breaches.

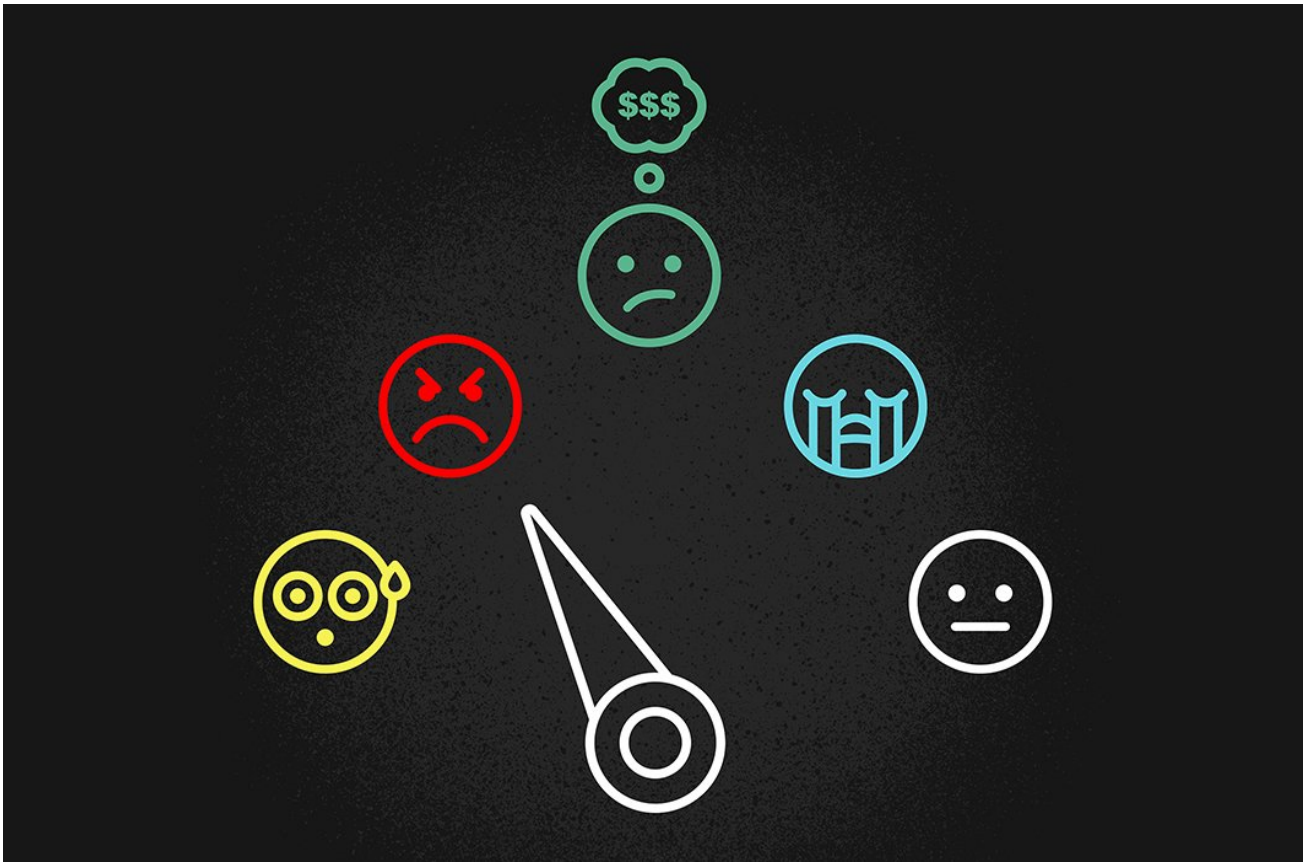
Additional Resources

- *Learn more about COZY BEAR in the CrowdStrike Adversary Universe.*
- *Download the CrowdStrike 2021 Global Threat Report for more information about adversaries tracked by CrowdStrike Intelligence in 2020.*
- *See how the powerful, cloud-native CrowdStrike Falcon® platform protects customers from DarkSide ransomware in this blog: DarkSide Goes Dark: How CrowdStrike Falcon Customers Were Protected.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*

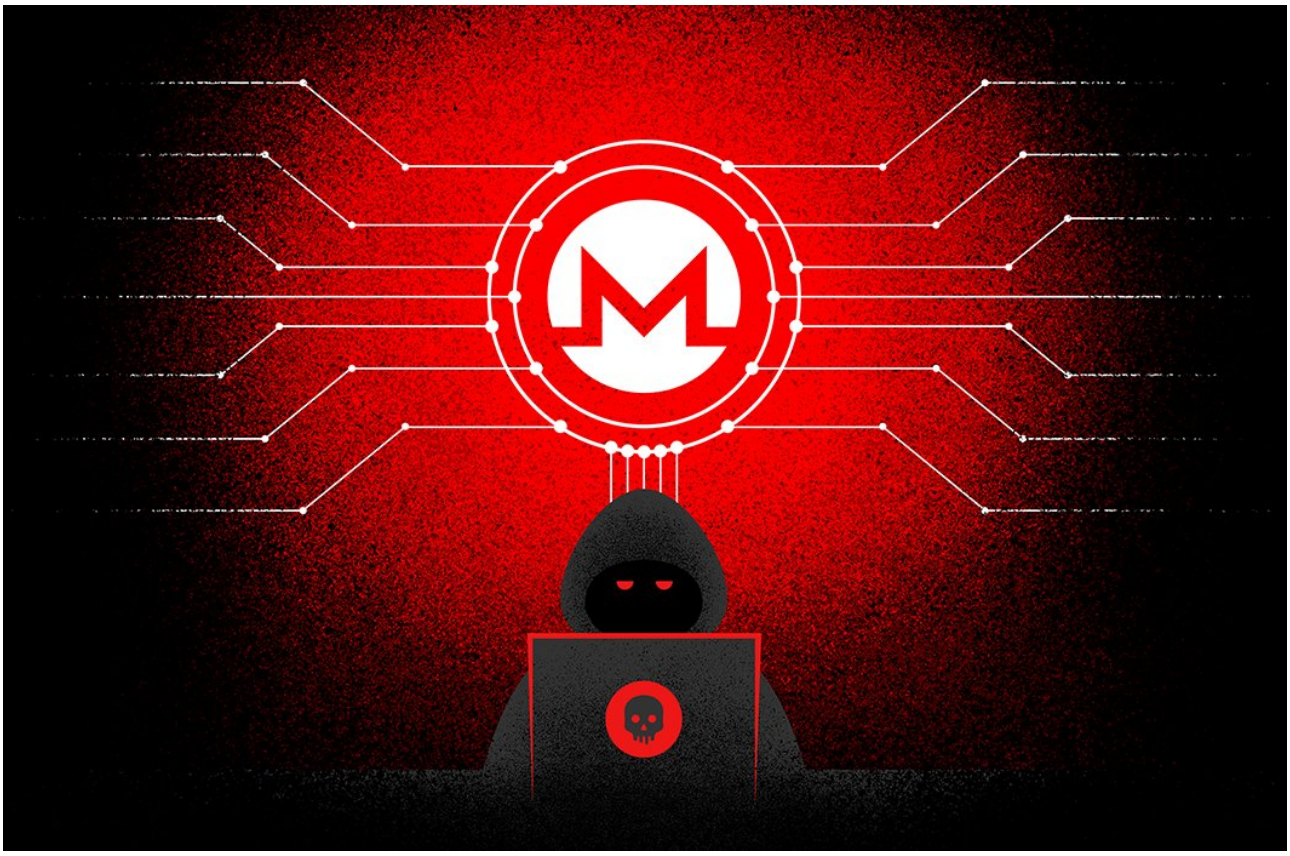
Related Content



Compromised Docker Honeypots Used for Pro-Ukrainian DoS Attack



Navigating the Five Stages of Grief During a Breach



LemonDuck Targets Docker for Cryptomining Operations