2021 Global Attitude Survey Takeaways

crowdstrike.com/blog/better-together-global-attitude-survey-takeaways-2021/

Falcon OverWatch and Falcon Complete teams January 21, 2022

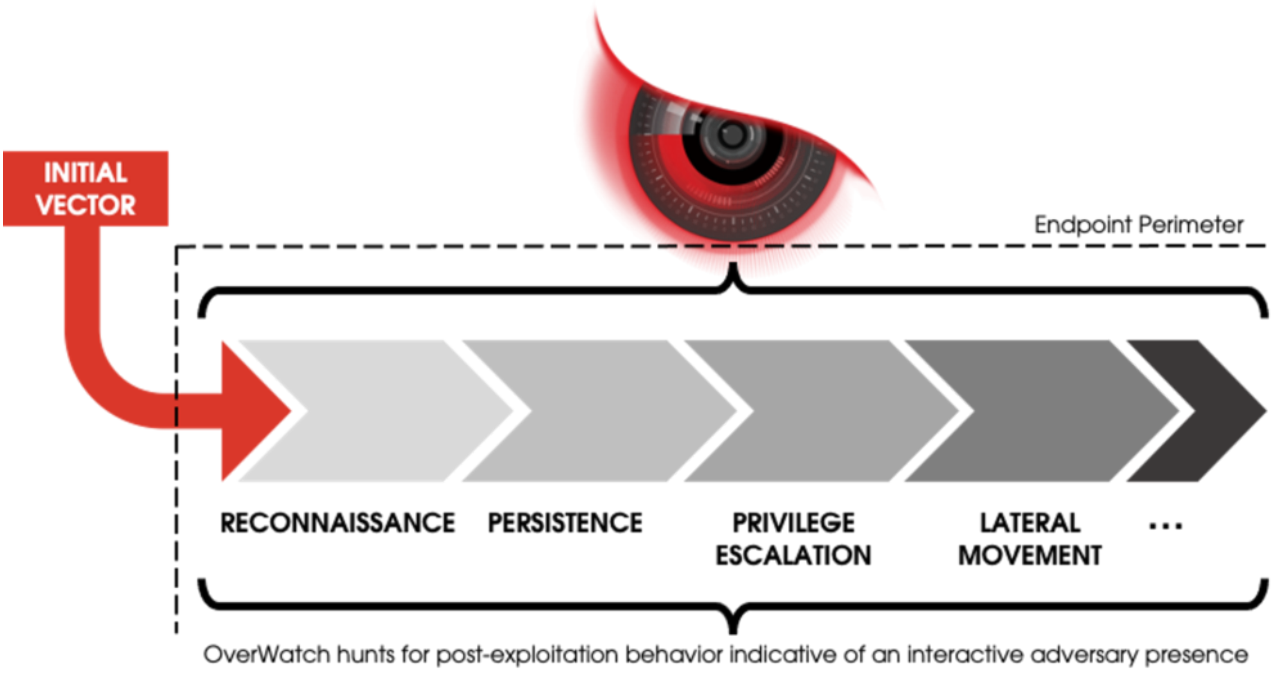
The results from the 2021 Global Security Attitude Survey paint a bleak picture of how organizations globally are feeling about the cybersecurity landscape before them. Organizations are grappling with shortages of cybersecurity skills and a lack of capability to detect and contain intrusions in a timely way. This comes against a backdrop of persistent ransomware attacks, the increasing regularity of supply chain vulnerabilities and a large attack surface due to sustained high levels of remote work.

Although these are legitimate concerns, the battle is not lost. Effective managed cybersecurity services that include continuous threat hunting and rapid response can provide organizations with an immediate injection of world-class capability to detect, disrupt and contain serious hands-on-security threats at speed and at scale.

"Trusted" Entry Points Are No Match for Human Hunters

Many survey respondents (84%) predict that supply chain attacks could become one of the biggest cyber threats facing their organization. This boils down to a fear of an adversary gaining access through a trusted channel and going undetected. Sophisticated attacks of this

nature require a mix of automation and human expertise in the form of human-based threat hunting. One of the strengths of threat hunting is that the ability to quickly and decisively detect a threat is not contingent on the initial access vector. Whether initial access is achieved via a supply chain attack, a vulnerable public-facing application or another trusted entry point, CrowdStrike Falcon® OverWatch™ remains vigilant in hunting for post-exploitation behavior that signals an interactive threat on an endpoint.



OverWatch recently uncovered interactive intrusion activity that followed the unintended download of a suspected backdoored Zsh installation file. Zsh is a legitimate Unix shell and was likely downloaded by the victim organization from a legitimate GitHub repository.

Upon download and installation of Zsh, a binary for the remote access utility NetSupport was executed. Concurrently, the malicious installer also attempted to download additional binaries and batch files from an external domain. OverWatch tracked the adversary as they leveraged NetSupport to execute PowerShell commands to download a malicious DLL and batch file from an adversary command-and-control (C2) server and execute basic network reconnaissance commands. Later investigation found that the malicious DLL was modified to include VBScript that, if loaded, would have attempted to disable and add a number of folder exclusions to a third-party security tool.

This attempted intrusion highlights how adversaries abuse user trust in legitimate download locations and exploit public edit settings on numerous GitHub repositories. Fortunately for this victim organization, OverWatch's continuous hunting quickly spotted the anomalous activity based on threat hunting leads and known indicators of compromise (IOCs). Based on this rapid detection, OverWatch provided the necessary context to the victim organization enabling them to take swift remedial action.

Managed threat hunting delivers the human element that is crucial in detecting and disrupting adversary activity designed to exploit trusted components in a victim environment. Unlike solutions based exclusively on automated technology, human hunters approach their analysis with informed skepticism. OverWatch looks for behaviors that are indicative of a malicious presence in an environment. While the application or user activity involved with initial access might fall within parameters that technology considers normal, hunting looks at the broader context to detect even the faintest traces of malicious follow-on activity.

OverWatch and Falcon Complete Combine Forces to Stop Ransomware in Its Tracks

The 2021 survey also revealed that the persistent threat of ransomware attacks remains organizations' most pressing cybersecurity concern, a concern that is firmly based in their lived experience. Two-thirds of the organizations surveyed had fallen victim to at least one ransomware attack in the preceding 12 months. This highlights how critical it is for organizations to have comprehensive security solutions in place that ensure that ransomware attempts are met with swift and decisive action.

OverWatch and CrowdStrike Falcon® Complete™ recently disrupted a ransomware attempt against a victim organization's domain controller. An affiliate of the LockBit ransomware as a service (RaaS), run by BITWISE SPIDER, targeted the domain controller by exploiting the Zerologon vulnerability. The adversary connected to the domain controller remotely from a host on the network that did not have Falcon coverage. Thanks to the Falcon platform's rich telemetry on covered workloads and OverWatch's proactive threat hunting, the attack was immediately detected. Within minutes, OverWatch identified the adversary's presence and began investigating.

Having leveraged the exploit to obtain domain admin privileges, the adversary undertook initial discovery actions and created a new domain account to facilitate persistence and lateral movement. In under 20 minutes, the adversary used their new domain account to move laterally, via RDP, to another domain controller on the network, where they changed the "administrator" account's password. By this time, OverWatch hunters were already in direct communication and coordination with Falcon Complete responders to begin stopping the attack.

Less than 10 minutes after the breakout, the adversary deployed and attempted to execute a novel binary. Further analysis performed by the CrowdStrike Intelligence team found the binary to be a variant of LockBit 2.0. Thanks to the Falcon platform's prevention capabilities, the attempted LockBit execution was prevented, ensuring that this CrowdStrike customer did not become another one of BITWISE SPIDER's many victims.

A Bit About LockBit

> LockBit is developed by an adversary that CrowdStrike Intelligence tracks as BITWISE SPIDER, who provides their ransomware to affiliates in a RaaS model. BITWISE SPIDER has recently and quickly become a significant player in the big game hunting (BGH) landscape. Their dedicated leak site (DLS) has received the highest number of victims posted each month since July 2021 compared to other adversary DLSs due to the growing popularity and effectiveness of LockBit 2.0.

The Falcon platform is finely tuned to identify known malicious behaviors associated with ransomware. Despite the novel nature of the binary used in this attempted intrusion, the Falcon platform anticipated and immediately prevented the unknown threat from executing using a combination of artificial intelligence, behavioral detection and machine learning algorithms.

Meanwhile, OverWatch tracked the adversary at every turn, providing context-rich information about the adversary's movements to Falcon Complete, whose responders notified the customer and rapidly performed their response. Falcon Complete began by rapidly network containing the affected hosts, completely cutting off the adversary's remote access. They also disabled the domain account created by the adversary and deployed a custom IOC hash block across the entire environment for the observed LockBit variant. To further assist the customer, Falcon Complete analysts delivered specific recommendations for further hardening of the network, including guidance, removing the adversary-created account, resetting the affected "administrator" account and fully patching the compromised domain controller.

Thanks to the unrivaled security combination of the Falcon platform and the OverWatch, CrowdStrike Intelligence and Falcon Complete teams, the adversary was thwarted. This coordinated response effectively stopped the intrusion before the customer suffered any significant impact — protecting them against a serious eCrime threat that is growing all too prevalent.

The findings from last year's survey prove that it is a matter of when, not if, an organization will fall victim to an attempted ransomware attack. Yet, respondents' self-reported estimated time to detect an intrusion has increased to an average of 146 hours, or over 6 days. Having expert managed services on your side makes the difference when minutes matter. The combination of OverWatch's unrivaled ability to uncover adversary activity and Falcon Complete's expert and timely response is proven to disrupt ransomware attempts before the adversary can do damage.

Managed Services Plug the Skills Gap

Amid these persistent threats, organizations report difficulty in finding staff with the skills needed to establish and maintain a comprehensive security posture. Managed services can deliver an immediate injection of security capability that can begin to pay dividends from Day

One. In fact, OverWatch regularly uncovers pre-existing intrusions during roll-out to new customer environments.

CrowdStrike's managed services provide benefits that cannot easily be replicated with an in-house solution. Because CrowdStrike analysts have access to cloud-scale telemetry encompassing trillions of events per day, they have unparalleled visibility across the entire customer install base. This allows hunters to rapidly identify anomalous activity, which ensures every customer benefits from near-real time insights into active threats. Both OverWatch and Falcon Complete are powered by CrowdStrike's global threat intelligence, bringing critical context to the detection and response process. Crucially, all of this is delivered with 24/7/365 coverage, providing comprehensive security when it is most needed: ALWAYS.

Finally, a partnership with CrowdStrike's managed services equips organizations with round-the-clock access to elite resources. OverWatch's expert hunters deliver context-rich alerts that empower organizations to rapidly contain threats and remediate their environments with confidence. For organizations leveraging the power of Falcon Complete, expert responders will work in lock-step with OverWatch threat hunters to rapidly and surgically remediate malicious activity on an organization's behalf.

Managed services can be your fast track to a comprehensive, mature endpoint security program that equips you to face the most pressing global security challenges into 2022 and beyond.

Additional Resources

- *Download the 2021 CrowdStrike Global Security Attitude Survey.*
- *Learn more about Falcon OverWatch's proactive managed threat hunting.*
- *Check out the Falcon Complete product webpage.*
- *Watch this video to see how Falcon OverWatch proactively hunts for threats in your environment.*
- *Read a white paper: CrowdStrike Falcon® Complete: Instant Cybersecurity Maturity for Organizations of All Sizes.*
- *Learn how the powerful CrowdStrike Falcon® platform provides comprehensive protection across your organization, workers and data, wherever they are located.*