Exploit Research Strengthens Customer Protection

crowdstrike.com/blog/exploit-research-strengthens-customer-protection/

Joseph Goodwin - Aspen Lindblom February 22, 2022

- CrowdStrike continuously observes and researches exploit behavior to strengthen protection for customers
- Code execution techniques constantly target Windows, Linux and macOS operating systems
- Successful remote/arbitrary code execution can enable a foothold for attackers to continue compromise
- Understanding and detecting post-exploit activity is imperative for keeping environments safe

As technology continues to evolve rapidly, so do the techniques used by adversaries. This may be considered a given, but it is important to appreciate how attackers may leverage existing and commonly used applications within an environment to attempt to seize control and achieve their objectives. These post-exploitation tactics are something that the CrowdStrike Falcon® sensor homes in on and detects, generating alerts when it observes a process acting suspiciously, to ensure our customers are alerted and kept up-to-date with precisely what is happening in their environments.

In most cases, an attacker will attempt to gain some form of code execution — either arbitrary code execution (ACE) or remote code execution (RCE) — to further their reach into an environment and achieve their objectives. If an adversary obtains code execution in a targeted environment, they have succeeded in gaining a foothold to continue their attack. How they choose to continue is determined by their end objective. For example, some common next steps may include reconnaissance, privilege escalation, information stealing, or dropping and executing further payloads. The impact that this may cause can only truly be measured by the victim after the damage has been done, but suffice to say, it is never a positive situation for any company.

CrowdStrike takes a layered approach to security to detect and prevent post-exploit activity, such as attempted malicious code execution throughout these multiple layers. It is important to understand that the concepts of ACE and RCE are not bound to a specific operating system (although particular instances will be). This is why we research and simulate vulnerabilities — to provide customers with the best available defense against exploitation of vulnerabilities delivered through these types of attacks.

To help illustrate the Falcon platform's diversity in its ability to detect these types of unwanted code-execution vulnerability attacks, this blog discusses examples of both RCE and ACE vulnerabilities in Windows, Linux and Mac. We take a deep look into how the Falcon sensor identifies these threats to keep your environment safe.

Windows: Microsoft MSHTML Remote Code Execution Vulnerability

In Windows, there are RCE vulnerabilities that affect the MSHTML browser engine. Attackers can create malicious Microsoft Office documents exploiting these vulnerabilities, and then trick users into opening them. In essence, attackers place a special object within a document file. When the victim opens the tainted document, an attacker-controlled external URL is contacted, and its contents are downloaded and subsequently executed by the MSHTML engine.

At the time of its disclosure, this vulnerability was reported to have been observed being exploited in the wild. Microsoft has stated that MS Office opens documents in Protected View or Application Guard for Office, therefore providing some form of prevention against the exploitation of the vulnerability. However, if an attacker is able to craft a document which the user trusts and in turn, enables editing, the vulnerability may be exploited.

Customers taking advantage of our Spotlight service are able to input CVEs (such as this one) and get results returned on endpoints that may be vulnerable to the related types of attack. Also provided is a wealth of information in relation to the CVE and required steps for remediation. One of the links provided within a Spotlight scan for a CVE is a link to the vendor advisory for further reading. In the case of this example the related advisory published can also be found here.

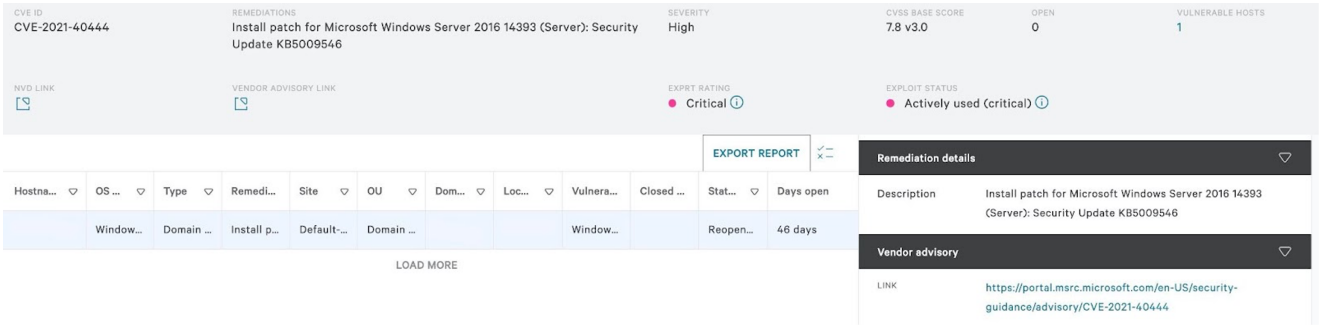

Figure 1. Spotlight returns results of hosts vulnerable to CVE-2021-40444 (Click to enlarge)

Additionally, after in-depth testing to replicate how these vulnerabilities are triggered, common patterns emerge regarding the process trees generated from exploiting them.

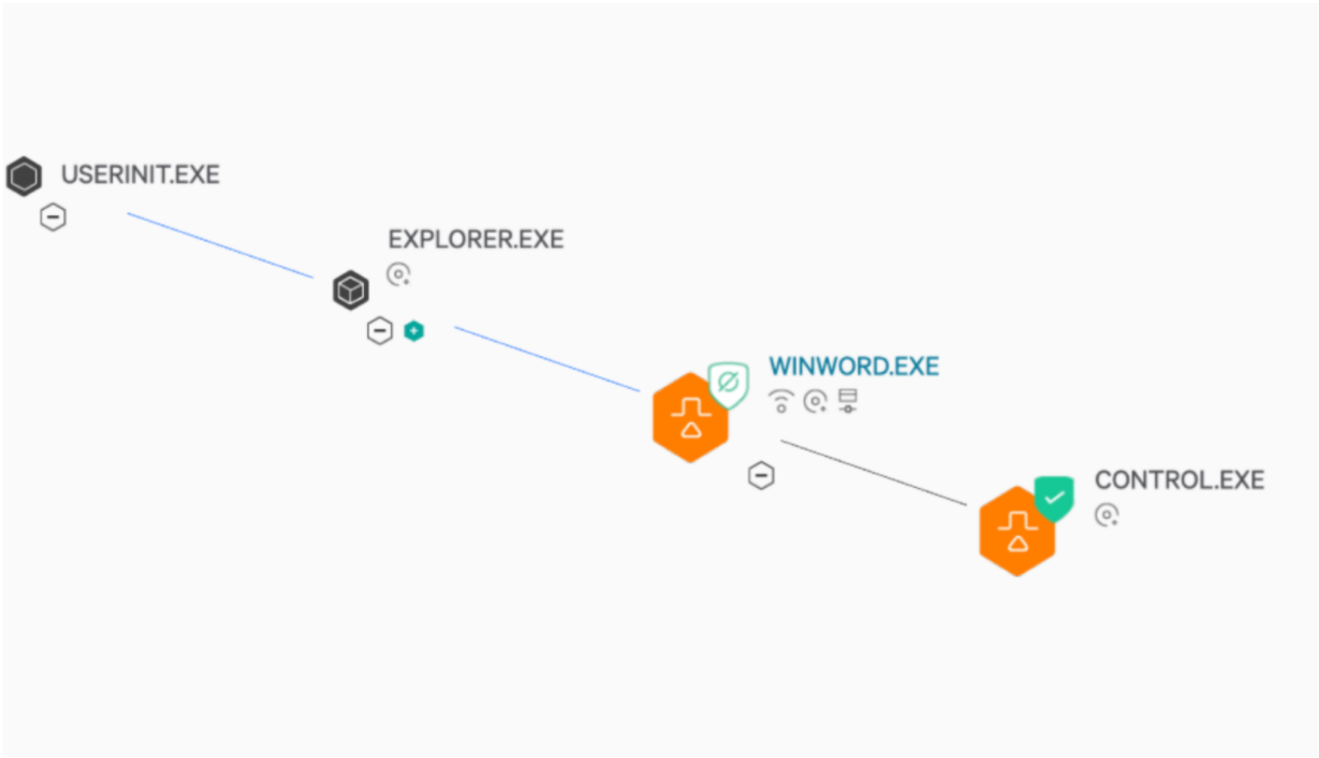

Figure 2. Falcon process tree for MSHTML browser engine remote code execution (Click to enlarge)

This included activities like productivity applications writing binaries with unique, targetable values such as file name, file type or behavior. Discovering this ensured that the relevant detection research teams could target several different levels of the process trees, which, when all seen together, indicated this RCE attempt in a myriad of different scenarios.

Even after the initial work had been conducted (and the associated detections released), further analysis uncovered additional areas throughout the kill chain that yielded high true positive detection rates for activity relating to this RCE behavior. This subsequent analysis uncovered specific file types being written to targeted locations on disk which matched a unique process lineage. For the best possible coverage for customers, this avenue was further explored and confirmed to indicate behavior associated with MSHTML browser

engine RCE. As a result of this research, multiple detections were pushed out to all customers to form a multi-layered defense against exploitation attempts for this vulnerability and ensure that customers are protected.

Linux: Targeted Arbitrary Code Execution in Specific Server Types

One example of a Linux vulnerability involves Object-Graph Navigation Language (OGNL) injection in specific server types and data center software. For instance, a specially crafted request can be sent to vulnerable endpoints on the associated server or data center instance. Furthermore, this could be exploited by either a remotely authenticated attacker or, under the right circumstances, an unauthenticated attacker, which would lead to arbitrary code execution, potentially raising the severity of the vulnerability to critical.

After its initial public disclosure on August 25, 2021, the CrowdStrike Falcon OverWatch™ threat hunters began to relentlessly investigate any implication that CrowdStrike's customers may be under attack via this method. Through their investigations, the associated teams quickly began to see the attack surface for this vulnerability widen from purely Linux-based exploitation attempts to including Windows attempted exploitation.

With their knowledge of the exploit and their observations on attempted attacks against customers, OverWatch hunters were quick to identify early signs of attempted exploitation. One such example includes attackers writing and decoding a Base-64 encoded string to a file in the confluence directory. You can read more on the Falcon OverWatch hunting team's efforts here.

Due to the severity of this vulnerability, other internal teams also began performing parallel research efforts to ensure that CrowdStrike's scope of coverage against this vulnerability ensured maximum coverage. These scenarios are thoroughly researched and tested in controlled environments to obtain as much relevant telemetry as possible. This way, the research teams can find patterns related to the behavior of the exploit and determine ways in which the Falcon sensor's layered approach can detect it. Specific points of interest can emerge, such as similarities in the process lineage itself, the associated command lines used on each level, and specific behavioral traits displayed by the endpoint.

By reviewing the telemetry and associated process trees in successfully exploited scenarios, the teams can craft detections based on both patterns that emerge in the process trees and observed behavior displayed by the endpoint. This helps further reduce false positive detections and strengthens the probability that the associated activity relates to exploiting a known vulnerability. Associated exploit activity observed in testbed detonations included various attempts at persistence, network connection activity, recon activity, and attempted file download, among many others. Targeting the process actions and its requests of the endpoint helps ensure that the CrowdStrike Falcon sensor produces high-fidelity detections for customers.

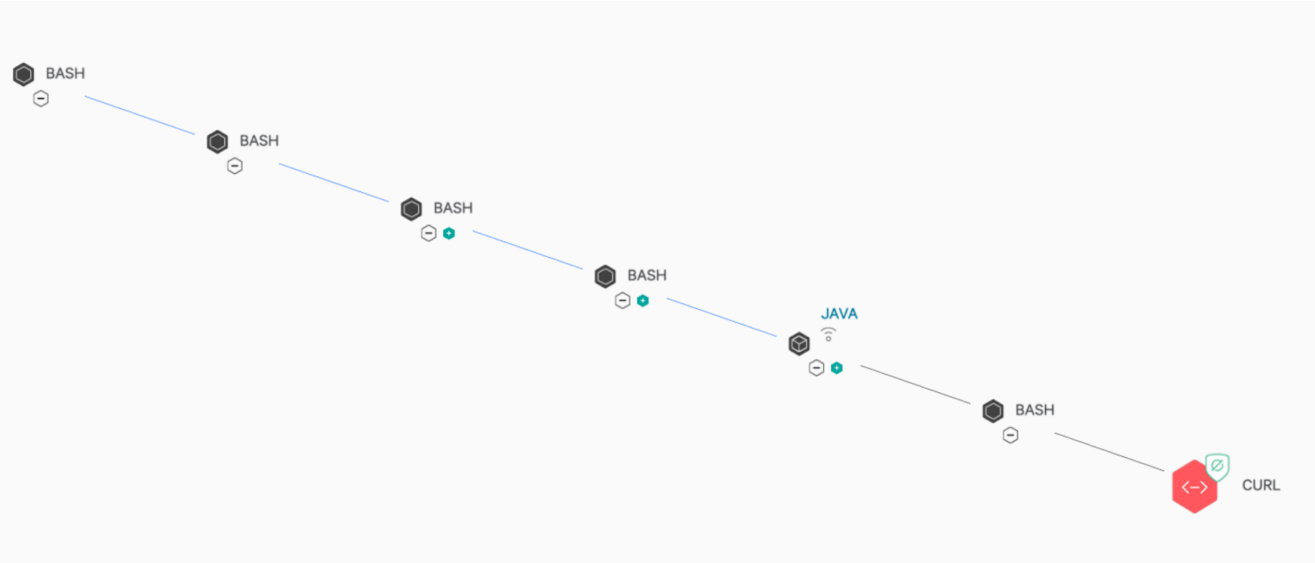

Figure 3. Falcon process tree for observing and killing malicious post-exploit behavior occurring on a vulnerable server (Click to enlarge)

What's interesting about the above screenshot (which shows the related activity being blocked) is that it highlights a common post exploit method where attackers often attempt to utilize wget/curl (etc.) in order to retrieve further payloads to run in targeted environments to extend their reach. This method is also seen with the more recent Log4j exploit attempts (shown in Figure 4) where CrowdStrike prevented the malicious actions from occurring.

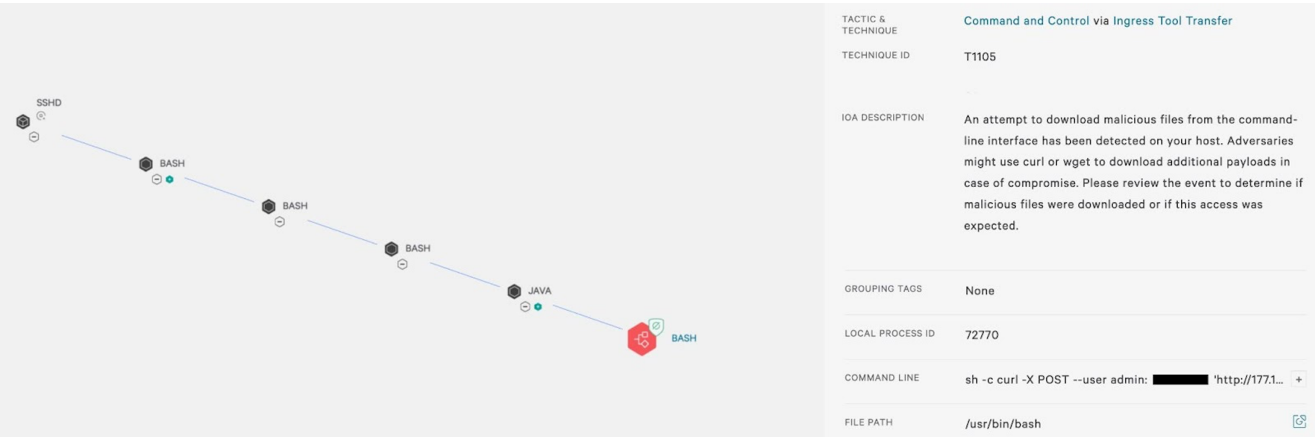

Figure 4. Process tree of post-exploit log4j attempted malicious download (Click to enlarge)

macOS: Pre-install Scripts

Another tactic using post-exploit code execution in macOS environments involves malicious post/pre-install of package scripts. In essence, malicious scripts leverage the macOS Installer API during an installation process. This type of behavioral manipulation is yet another avenue that attackers can exploit to gain a foothold into a network. While not technically considered a "full" RCE (as it still requires user interaction to run the initial install), this technique is another form of RCE that attackers can use to compromise an endpoint and subsequently a network.

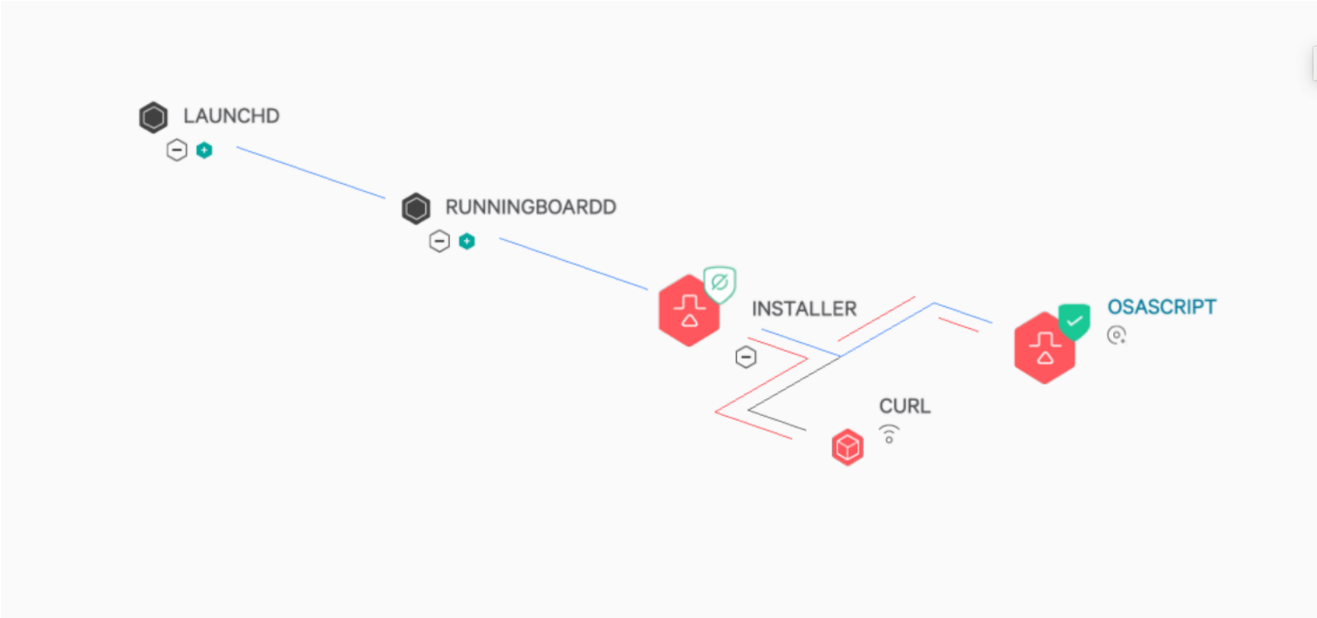

Figure 5. Falcon process tree for malicious pre-install package scripts (Click to enlarge)

For instance, Silver Sparrow is a malware example that uses this method. The user runs a seemingly innocent .pkg file and unknowingly triggers RCE, which can be used for persistence, connect to a command-and-control (C2) channel, perform active recon on the target machine or conduct other attacker-related activities.

The important thing to recognize here is that this malware is a pre-installer, which means that the code is run at the very beginning of the .pkg files execution. This means that the end user is already infected by the time the installation of the .pkg file has completed. Fortunately, the CrowdStrike Content Research and Response team was able to investigate and mitigate the associated behavior to ensure that this type of scenario does not play out in customer environments.

With the emergence of this technique, CrowdStrike's Content Research and Response team began investigating this activity to identify and prevent it within customer macOS environments. We quickly began to understand the methodology of the attack by reviewing existing telemetry and the associated data generated from further testing. After obtaining a thorough understanding of how this attack is conducted, and the risk which it could pose to customers depending on the potential weaponization, the team found a way to ensure that the associated activity is killed before it has a chance to execute. After rigorous testing, CrowdStrike's Content Research and Response team were then able to ensure high-fidelity preventions were put in place to combat this type of exploit attempt by targeting it at multiple stages of the process lineage.

The Ultimate Value of CrowdStrike's Threat Research and Layered Approach to Security

Vulnerability exploitation research enables CrowdStrike to protect customers better. Coupled with our on-sensor and in-the-cloud machine learning and behavior-based protection, the Falcon platform can detect threats and protect customers. As with most vulnerabilities, the best option is to ensure that systems across any environment are part of a good patch management plan. CrowdStrike Falcon Spotlight™ is a scanless, "always on" vulnerability management solution for all of the endpoints in your infrastructure shining insight into areas of your environment that may require further attention in order to ensure a strong security posture is maintained.

Using an example from the above scenarios, we can see how Spotlight comes in to assist with its ability to utilize scanless technology to determine which endpoints in your environment may be susceptible to specific vulnerabilities simply by searching the CVE ID. This specific CVE has an ExPRT rating of Critical and a severity of High. Reviewing the detections against this CVE provides a wealth of information including remediation details, vendor advisories, references, probable sources and much more. (ExPRT rating is based on a dynamic rating ML model, that may differ from traditional CVSS scores. Learn more here.)

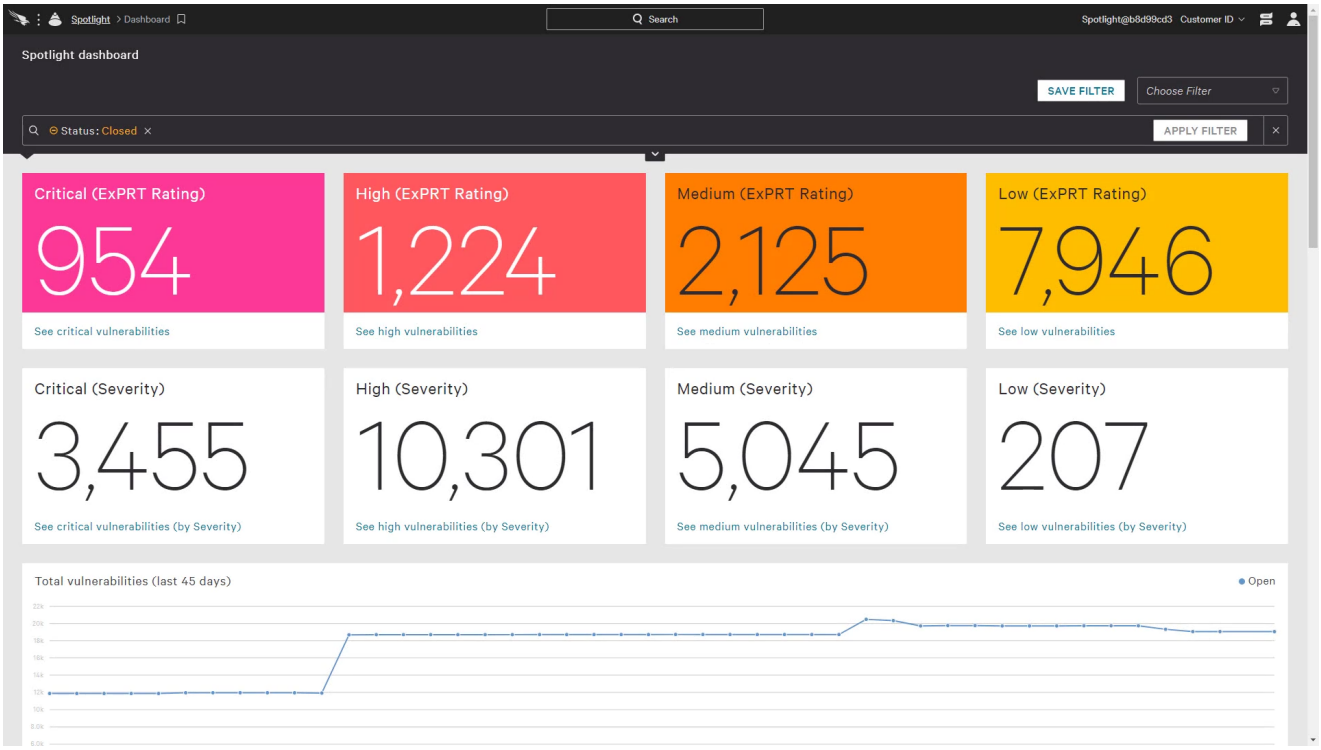

Figure 6. CrowdStrike Falcon Spotlight dashboard (Click to enlarge)

We can also see from the examples above how CrowdStrike's Falcon OverWatch threat hunters are quick to respond to an ever-evolving threat landscape, connecting the dots and piecing together critical bits of information to obtain the upper hand and keep our customers' environments safe.

Additionally, we can see how other teams such as Content Research and Response also investigate, analyze and create associated detections and preventions around suspicious activity — which has potential to cause significant harm into customer environments if used

under specific circumstances — while ensuring that related but benign activity is left to run unimpeded.

On top of all of this, there are *more* additional layers of security used, such as our various machine learning models which weren't even discussed.

The examples above describe how a technique, such as code execution, can come in various flavors across different operating systems and how CrowdStrike researchers investigate them to protect customers from exploitation and the multiple layers of protection we employ to ensure our customers' environments remain safe. We strive to ensure that our customers are kept safe from post-exploitation activity that could have a devastating impact if missed by adopting a layered approach to security. Attackers often find new ways to blend into environments, making it more challenging to detect their attempts to gain a foothold into endpoints and networks. At CrowdStrike, we remain dedicated to our mission to stop breaches.

Additional Resources

- *Read more about how Falcon protects against malware in this recent blog: CrowdStrike Falcon Proactively Protects Against Wiper Malware as CISA Warns U.S. Companies of Potential Attacks.*
- *Learn about the powerful, cloud-native CrowdStrike Falcon platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ to see for yourself how true next-gen AV performs against today's most sophisticated threats.*