THREAT INSIGHT

PowerShell Suspicious Scripting

Easing system administration tasks, while expanding the attack surface for cybercriminals: Get the benefits, without the headaches

For years, organizations and IT professionals have turned to Microsoft's PowerShell for its efficiency and ease of use.

It provides a well-integrated command-line experience for the operating system, and a simple way to manipulate server and workstation components. PowerShell is often treated as more secure than running most other scripting languages, and sometimes even treated as a 'trusted' application by security software and administrators.

Unfortunately, it has become increasingly common for cybercriminals to leverage PowerShell as a springboard into your organization and beyond. This abuse of legitimate tools like PowerShell is not new, but is on the rise as cybercriminals find new ways to use the tools combined with other tactics and techniques.

How is PowerShell used maliciously?

There are many attack types that frequently use scripting languages to carry out assaults on the endpoints. Two of the most common types, Living off the Land attacks and malware, often use suspicious PowerShell and cmd.exe scripts.

These scripting languages offer many easily implemented ways to obfuscate data, making automated analysis difficult. Many scripting attacks are constructed in a fragmented fashion such that each script is not malicious in itself - giving the perception that it may be 'safe'. Determining whether or not the fragmented attack is malicious requires evaluating many elements in the attack flow, and subsequently building an understanding of them so that patterns and markers can be established.

The power of machine learning and human intelligence

At ActZero, we protect systems and users from malware and attacks that abuse PowerShell and cmd.exe by continuously looking for suspicious scripts using our machine learning (ML) models. Our detections use ML anomaly detection coupled with domain knowledge to highlight unusual and suspicious looking scripts. Combined with human analysis of model predictions, this allows for the processing of large volumes of data and only notifying the end user when appropriate.

Anomaly detection: One of these things is not like the other

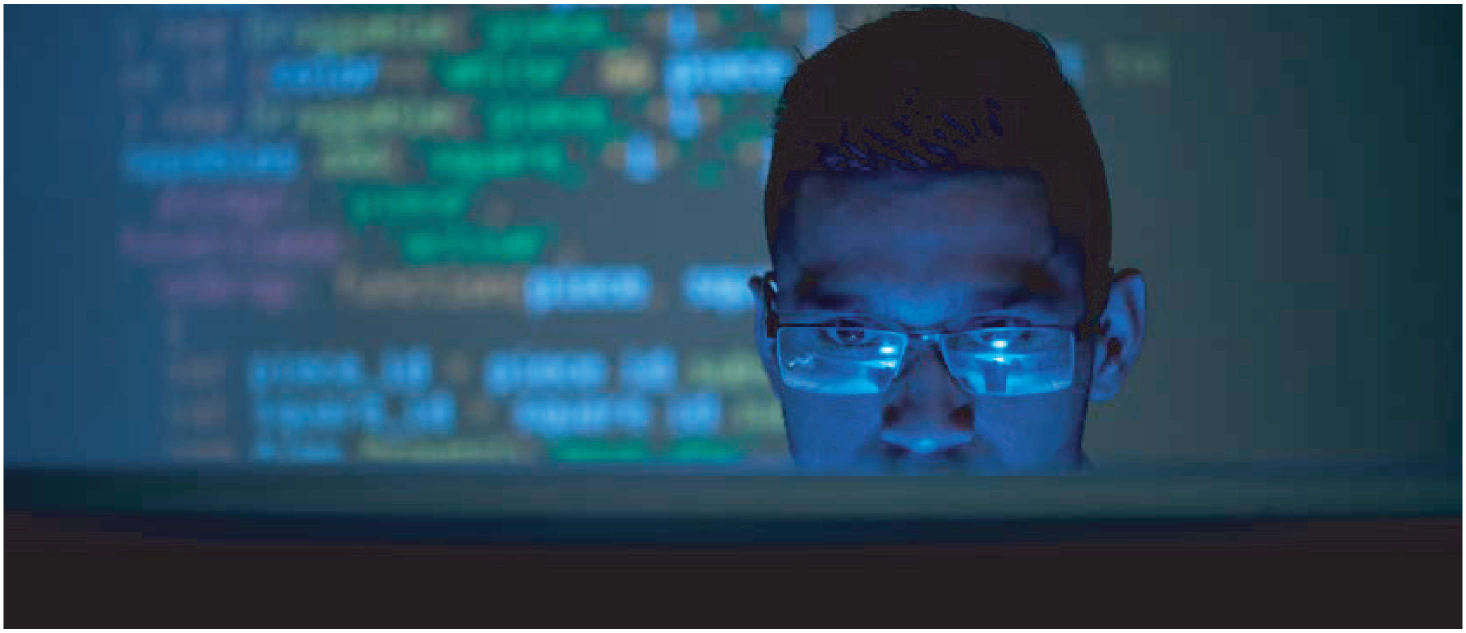
Organizations need a solution that is constantly monitoring their environment for multiple signs of abuse, especially those that are not obvious. The benefit of not simply looking for known markers is clear; You won't find the obscure if you're only looking for the obvious. Our machine learning is novel and successful because it is so generalizable. We use anomaly detection ML algorithms that provide many advantages over traditional single marker detection, including:

- Ranking the probability of a script being malicious by measuring how unusual the script is.
- Finding attacks that are novel and evade detection by rules based systems or even ML that is trained on known attacks. This allows our algorithms to even detect attacks that are specifically built to evade detection by simpler systems.
- Screening out scripts that include commands used in attacks, encoding, etc., but have been used by our customers before for legitimate purposes.

Our models look for the following features, as well as others:

- Methods used to obfuscate or encode command lines.
- Specific commands that have not been used frequently by our customers before.
- Command elements that are commonly used in attacks.

Analyzing these features on their own would make for poor heuristics. However, when utilized together in our ML models, and analyzed by our threat hunters, they provide valuable insight into the larger picture of what's happening in your environment.



Cyborg models: Human augmentation of machine learning

The success of these algorithms is not only rooted in their design, but also ActZero's humanin-the-loop system. Our team is constantly improving the machine learning models based on human labels and feedback on model output. Every time we catch a malicious script, relevant data from multiple data sources is analyzed and incorporated into the model if possible.

Armed with this data, our threat hunters know when and how to respond to suspicious scripts in our customers' networks, ultimately leading to enhanced protection for our customers against a large variety of cyberthreats.

Not yet a customer? Reach out now to our Sales team to learn more about our ActZero MDR offering, and our ransomware detection capability.