The Future of Cybersecurity

Bobbie Stempfley
Director, CERT Division

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0938

Evolving Challenges of Cyber

	Past	Present	Future
Threat and Vulnerability Landscape	• Simpler attack surface • Less connectivity • Fewer threat sources	Expanding attack surface More connectivity More threat sources	Adversary populations evolve: • AI and ML • biological computing • relentless auto-attacks
Barriers to Cybersecurity and Resilience	Static infrastructures require concrete defensive capabilities	Fluid virtual environments defended by humans, often third parties	Hyper-connected virtual environments defended by autonomous agents
Policies and Partnerships	DoD, law enforcement, information assurance policies, procedures, and controls	• Growth of federal cyber policies and strategies • Borderless collaboration with industry and international partners	• Adaptive national and international cybersecurity standards • International cyber-policy law

The Future Is Full of Paradoxes

- Zero-trust networks increase the need for trust in data
- The death of the boundary created a boundary explosion
- Smarter software requires safer and more secure infrastructure

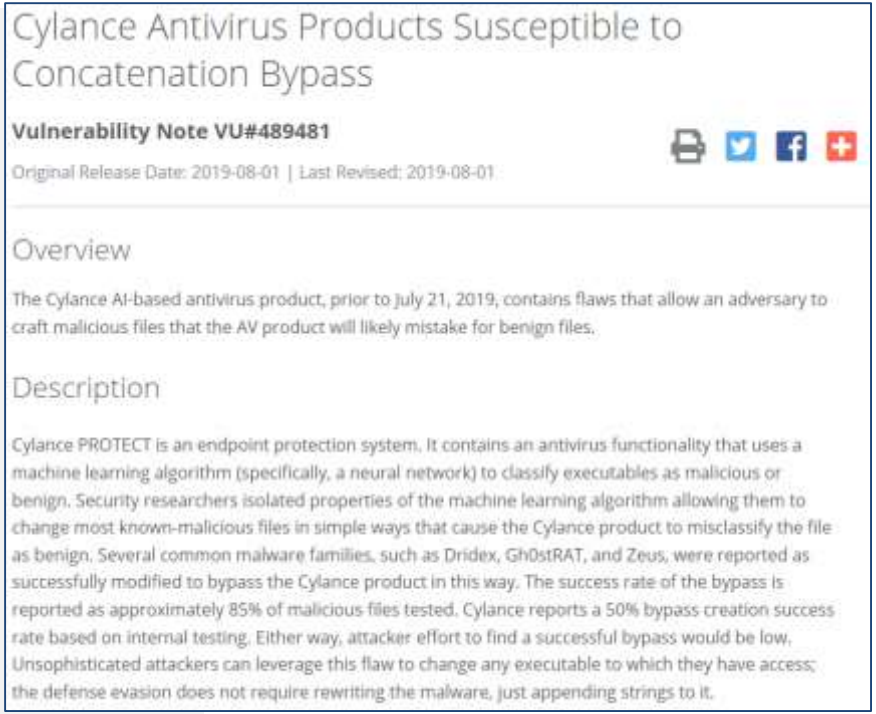
Zero-Trust Networks Increase the Need for Trust in Data

The Death of the Boundary Created a Boundary Explosion

Smarter Software Requires Safer and More Secure Infrastructure

Key Needs for the Future

- Verifiable confidence
- Next-generation cyber operations
- Trustworthy AI



Cylance Antivirus Products Susceptible to Concatenation Bypass

Vulnerability Note VU#489481

Original Release Date: 2019-08-01 | Last Revised: 2019-08-01

Overview

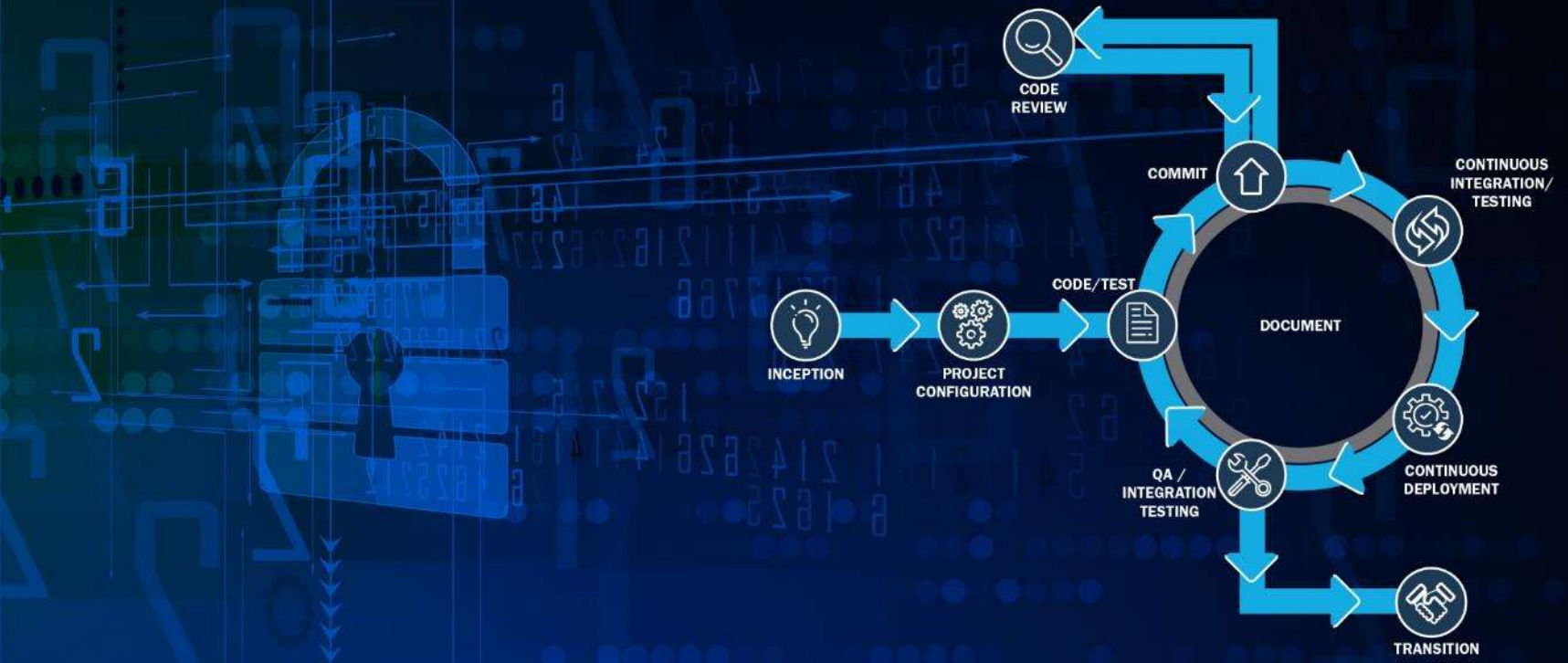
The Cylance AI-based antivirus product, prior to July 21, 2019, contains flaws that allow an adversary to craft malicious files that the AV product will likely mistake for benign files.

Description

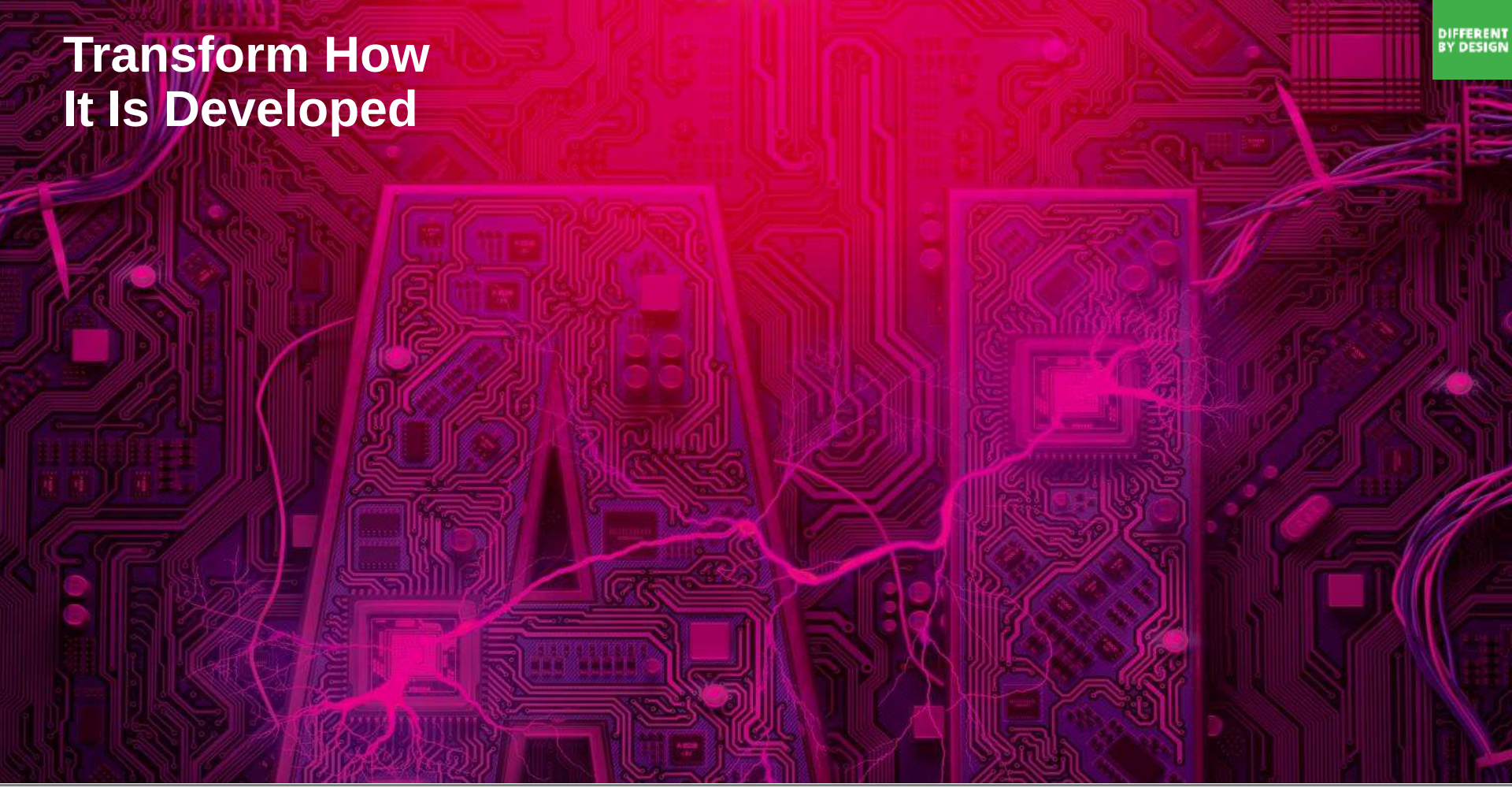
Cylance PROTECT is an endpoint protection system. It contains an antivirus functionality that uses a machine learning algorithm (specifically, a neural network) to classify executables as malicious or benign. Security researchers isolated properties of the machine learning algorithm allowing them to change most known-malicious files in simple ways that cause the Cylance product to misclassify the file as benign. Several common malware families, such as Dridex, Gh0stRAT, and Zeus, were reported as successfully modified to bypass the Cylance product in this way. The success rate of the bypass is reported as approximately 85% of malicious files tested. Cylance reports a 50% bypass creation success rate based on internal testing. Either way, attacker effort to find a successful bypass would be low. Unsophisticated attackers can leverage this flaw to change any executable to which they have access; the defense evasion does not require rewriting the malware, just appending strings to it.

Understand How to Test, Validate, and Recognize as Secure

Use DevOps and Secure DevOps

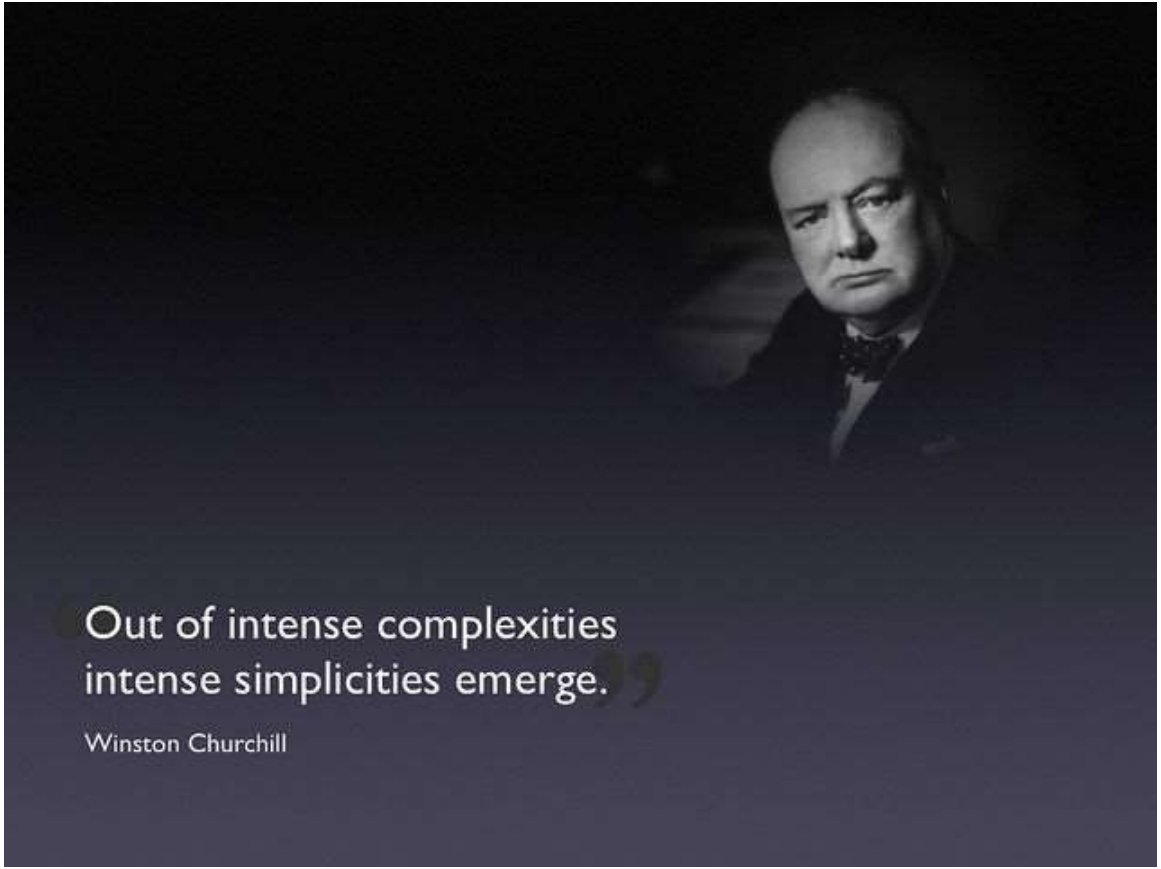


Transform How It Is Developed



Make It Secure from Inception

DIFFERENT BY DESIGN



Questions?