

The Future of Cybersecurity



Bobbie Stempfley
Director, CERT Division

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2019 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0938

Evolving Challenges of Cyber

	Past	Present	Future
Threat and Vulnerability Landscape	<p>Simpler attack surface</p> <p>Less connectivity</p> <p>Fewer threat sources</p>	<p>Expanding attack surface</p> <p>More connectivity</p> <p>More threat sources</p>	<p>Adversary populations evolve:</p> <ul style="list-style-type: none"> • AI and ML • biological computing • relentless auto-attacks
Barriers to Cybersecurity and Resilience	<p>Static infrastructures require concrete defensive capabilities</p>	<p>Fluid virtual environments defended by humans, often third parties</p>	<p>Hyper-connected virtual environments defended by autonomous agents</p>
Policies and Partnerships	<p>DoD, law enforcement, information assurance policies, procedures, and controls</p>	<p>Growth of federal cyber policies and strategies</p> <p>Borderless collaboration with industry and international partners</p>	<p>Adaptive national and international cybersecurity standards</p> <p>International cyber-policy law</p>

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.

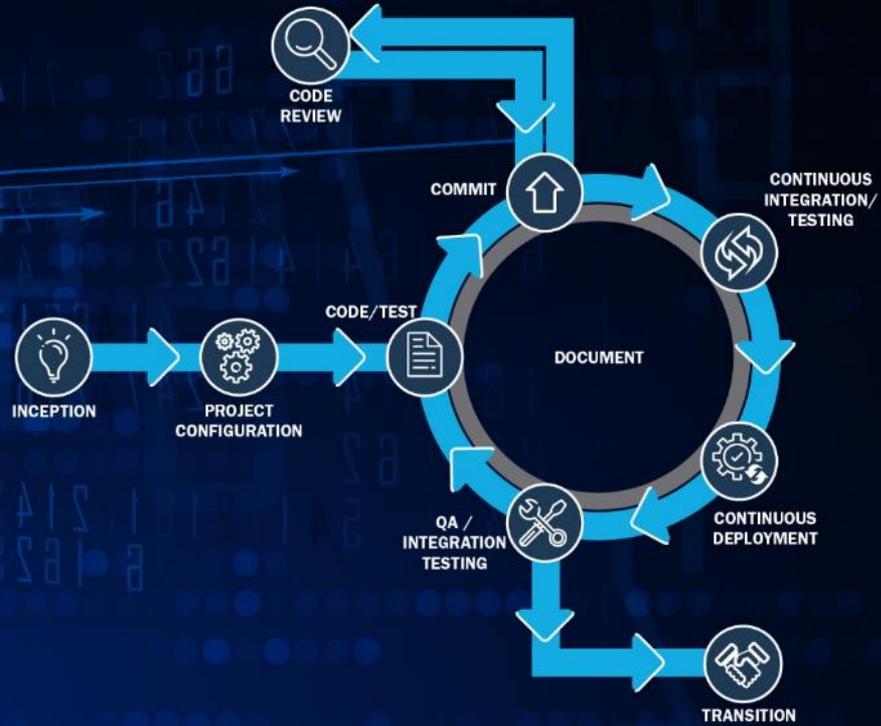
Description

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



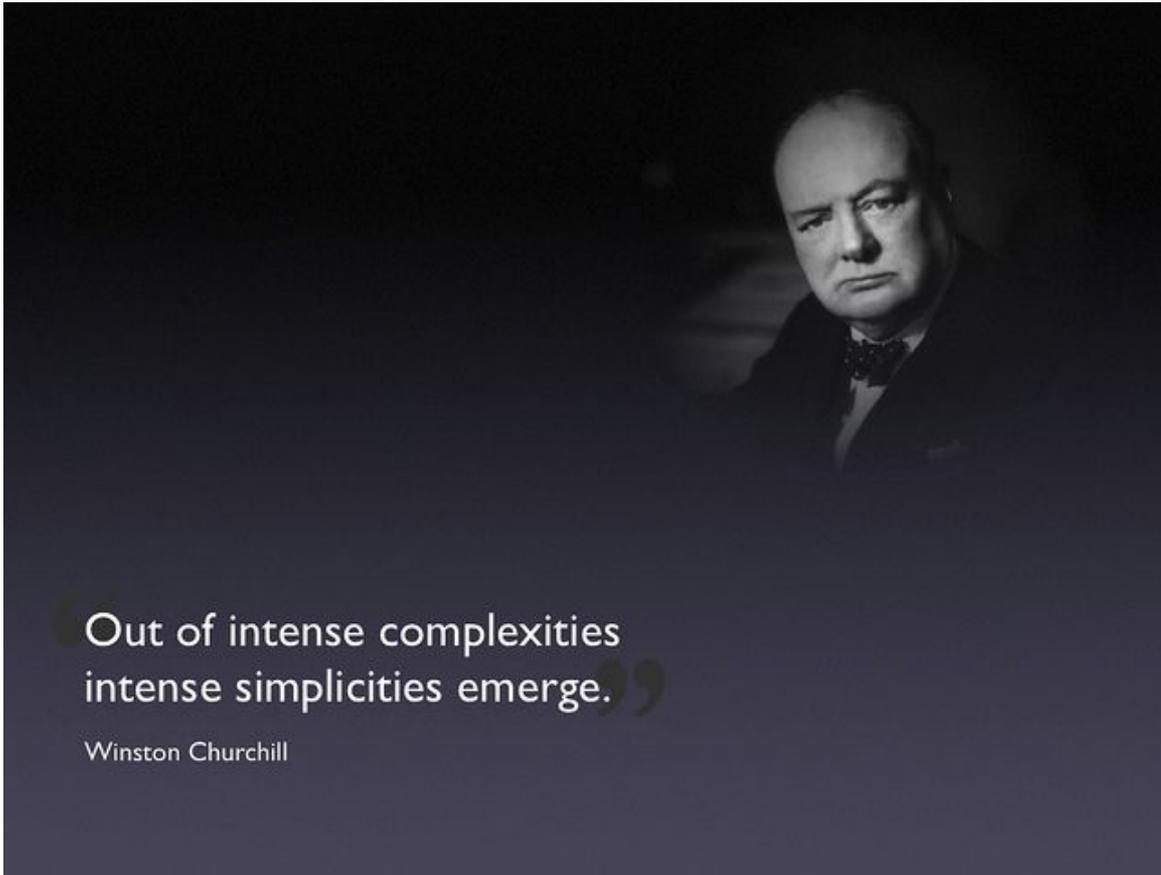
Use DevOps and Secure DevOps



Transform How It Is Developed

Make It Secure from Inception





“Out of intense complexities
intense simplicities emerge.”

Winston Churchill

For More Information

Bobbie Stempfley
Director, CERT Division

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213

Phone: 1+ 412-268-5800
Toll Free: 1+ 888-201-4479
Email: info@sei.cmu.edu

