NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

Pushing the Security Envelope

Presented by David Kennedy CEO / TrustedSec and Binary Defense

October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | #cybersummitmn

DAVE KENNEDY

OSCE, OSCP, CISSP, ISO 27001, GSEC, MCSE

Dave Kennedy is a computer hacker and the founder of TrustedSec and Binary Defense. Dave has helped with the Mr. Robot TV show as well as being directly mentioned on the show and others. Dave also served on the board of directors for the $(ISC)^2$ organization, is the co-author of the best-selling book "Metasploit: The Penetration Testers Guide", the creator of multiple widely downloaded open-source tools, frequent keynote speaker across the world and on the news, and an avid gamer.

Binary Defense

Managed Security Services

Security Information
and Event Management

Endpoint Detection
and Response

Counterintelligence

OUR MISSION

TrustedSec is an information security consulting team at the **forefront of attack simulations** with a **focus on strategic risk-management**.

Our goal is to help organizations defend against threats of all kinds and **change the security industry for the better.**


usa

The Beginning

- We are still finding our ways in security, but we are getting better.
- Still haven't been replaced by AI.
- What are the top 5 things that matter in security?

We are getting better.

- It's easy to say everything is broken.
- Harder to challenge the norm and work to make things better.
- The truth is we are getting better and we are maturing as an industry.
- Recognizing that not everything is broken and continue to drive to make things better.

#1 The Basics

- The basics are still kicking our butts today.
- Weak passwords, password management, 2FA, segmentation, application whitelisting, and more.
- Not an easy fix and takes time to change large business processes.
- Programs designed to try and handle everything.

Some Basics

- Prevention takes time however some high value ones:
  - Blocking unsigned executables in user profile directories as a start.
  - Constrained Language Mode.
  - Disallow regular users from PowerShell access.
  - PowerShell v6 and above.
  - Leverage ETW (Sysmon is a great start).
    - https://github.com/olafhartong/sysmon-modular
  - **Please, please, please** enable the Windows firewall internally.
- Detection can move faster:
  - You must, repeat must have endpoint logs.
  - Other sources such as DNS, east/west/north/south, command line auditing, script block logging, and more make a huge difference.
  - Visibility first, then improve on more visibility.
  - Understand the tactics and procedures attackers operate by vs. the techniques.
  - Threat hunting can help reduce the time window of a breach.

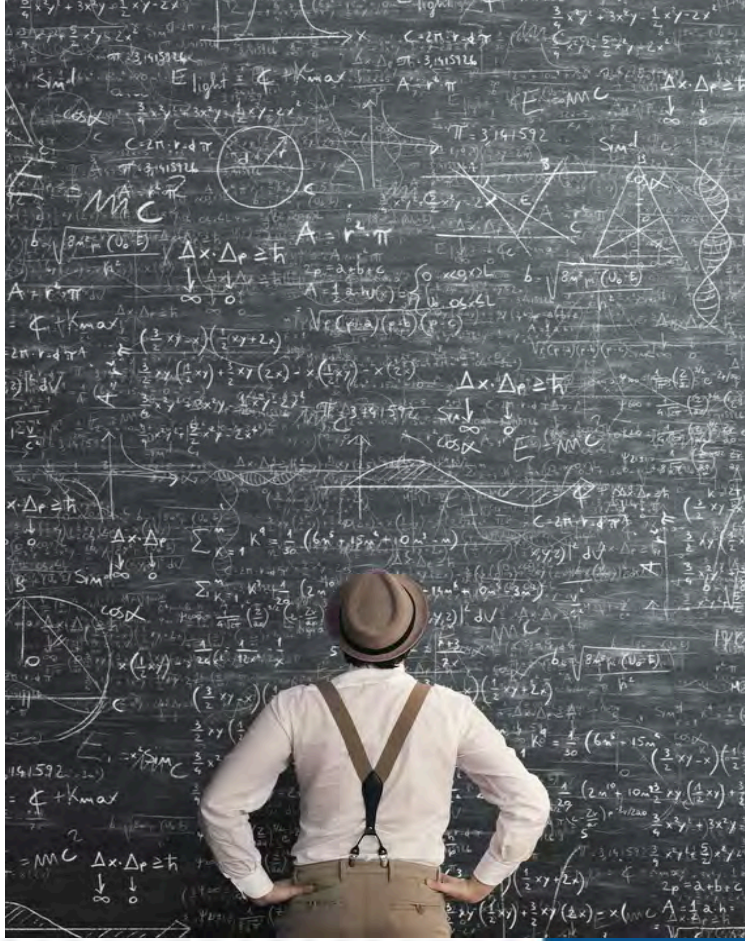
We purchase tools to try and fix poor security programs and lack of leadership.

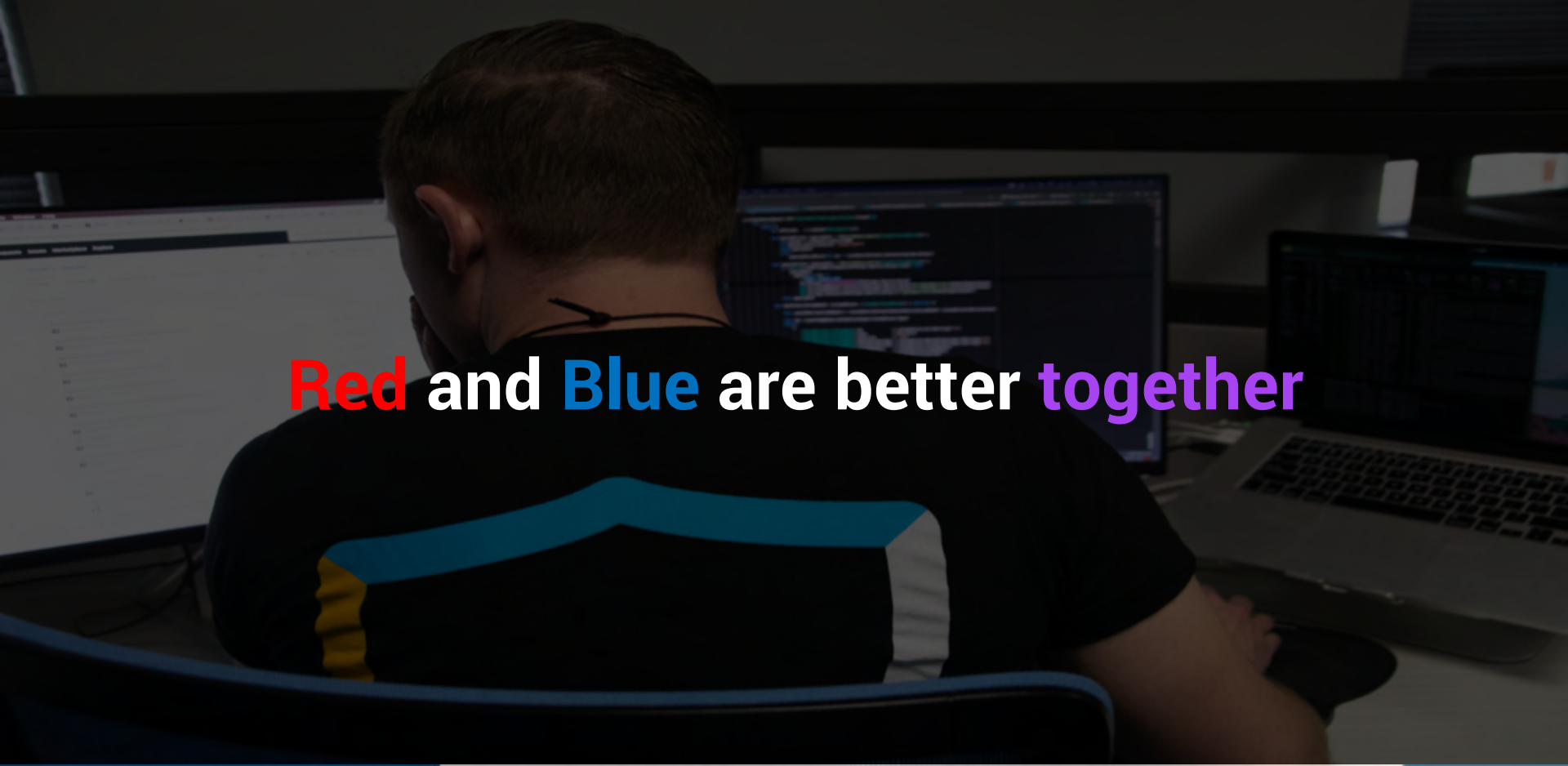
Most Organizations are at Basics

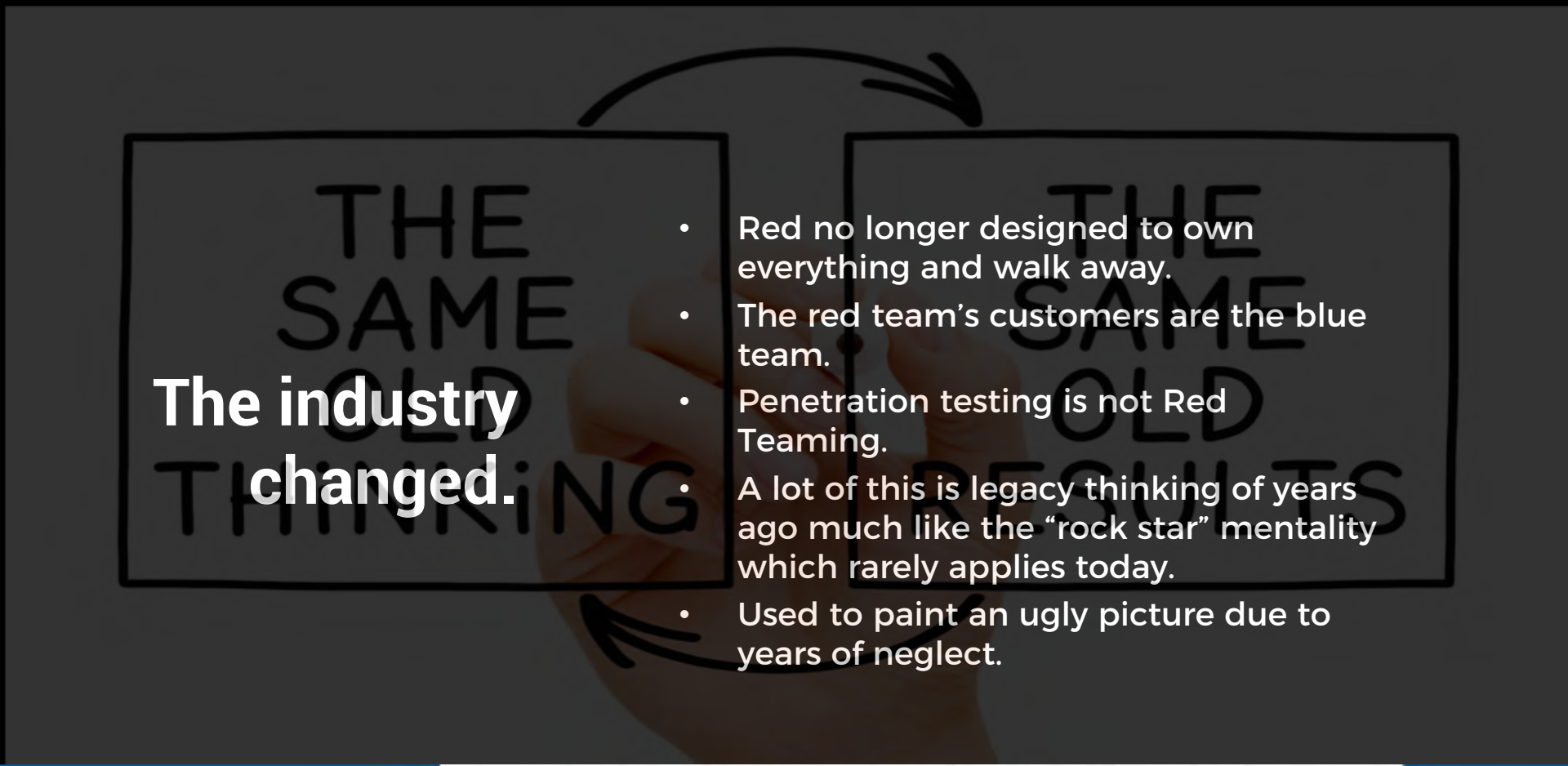
- Various reasons for this stem from executive buy-in, mismanagement, leadership, or infancy in security.
- Some are much further ahead than others.
- When working with companies that focus on collaboration, it's substantially harder for us as attackers.

#2 Simulations

- Tool releases are great for simulations.
- Without simulations, red and blue can't work together well.
- Working through identifying gaps in programs help put priority on what really matters.
- Usually companies don't even have the foundation for a building to build on this.




Red and Blue are better together

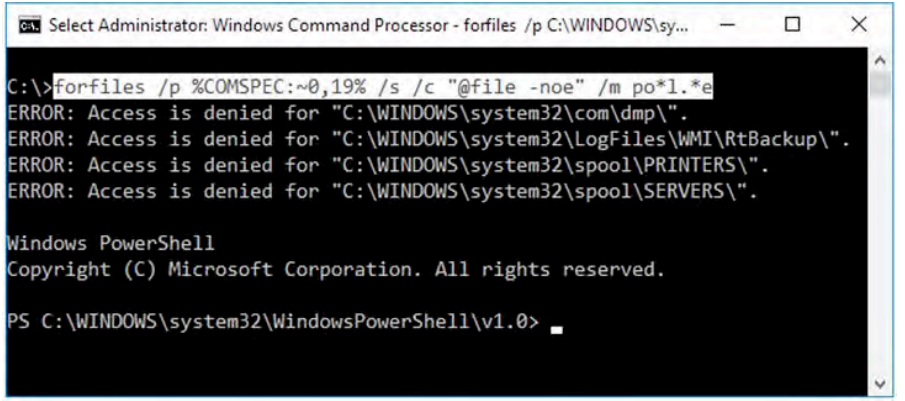


The industry changed.

- Red no longer designed to own everything and walk away.
- The red team's customers are the blue team.
- Penetration testing is not Red Teaming.
- A lot of this is legacy thinking of years ago much like the "rock star" mentality which rarely applies today.
- Used to paint an ugly picture due to years of neglect.

#3 Sharing and Collaboration

- More information shared now than ever.
- Still concerned about crowdsourced TTPs.
- Some Red Teams do their own research and customize tooling to compete.
- Red teaming has gotten harder.
- Research is a good thing.
- Releasing tools is a good thing.



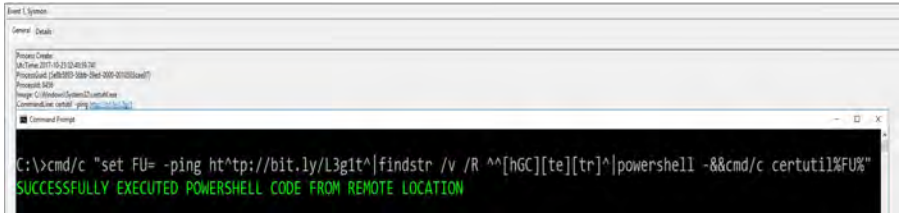


Image Sources: Daniel Bohannon @danielhbohannon (<3)

Sharing Between Groups

- Threat Hunting
  - Intelligence capabilities and unusual behavior.
- Red Teaming
  - Understanding capabilities of attackers and applying threat models and simulations.
- Security Operations Center
  - More than just alarm generation and responding to false positives.

- Blue Team
  - Working with a number of different teams to coordinate detection, response, or prevention.
  - While may not understand offensive capabilities, when given access to offense, substantially increases security of organization.
  - Vulnerability management probably these most important security program in an organization. (CMDB anyone?)

#4 Behavior

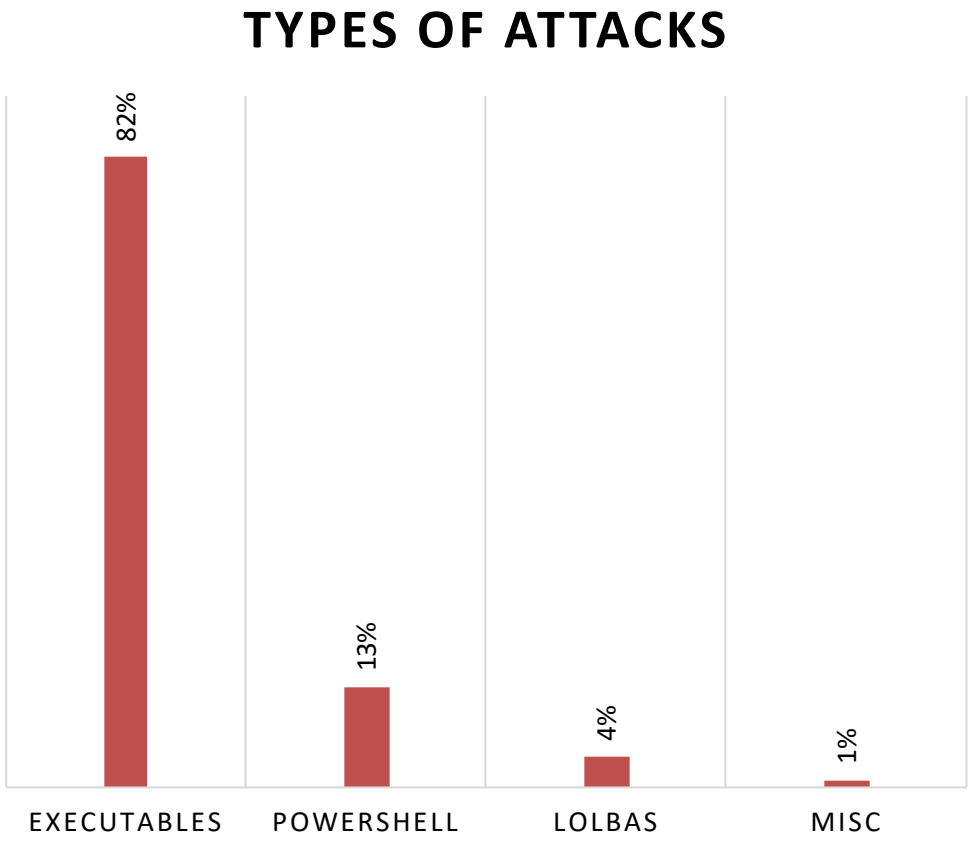
- We are focused on techniques, not tactics or procedures.
- Behavior creates too many false positives.
- Allocating appropriate resources for detection becomes challenging.

Visibility is Critical

- Protection takes time.
- Detection vs. Protection
- Visibility is first step and the most important one.
- This has to include endpoint logs.

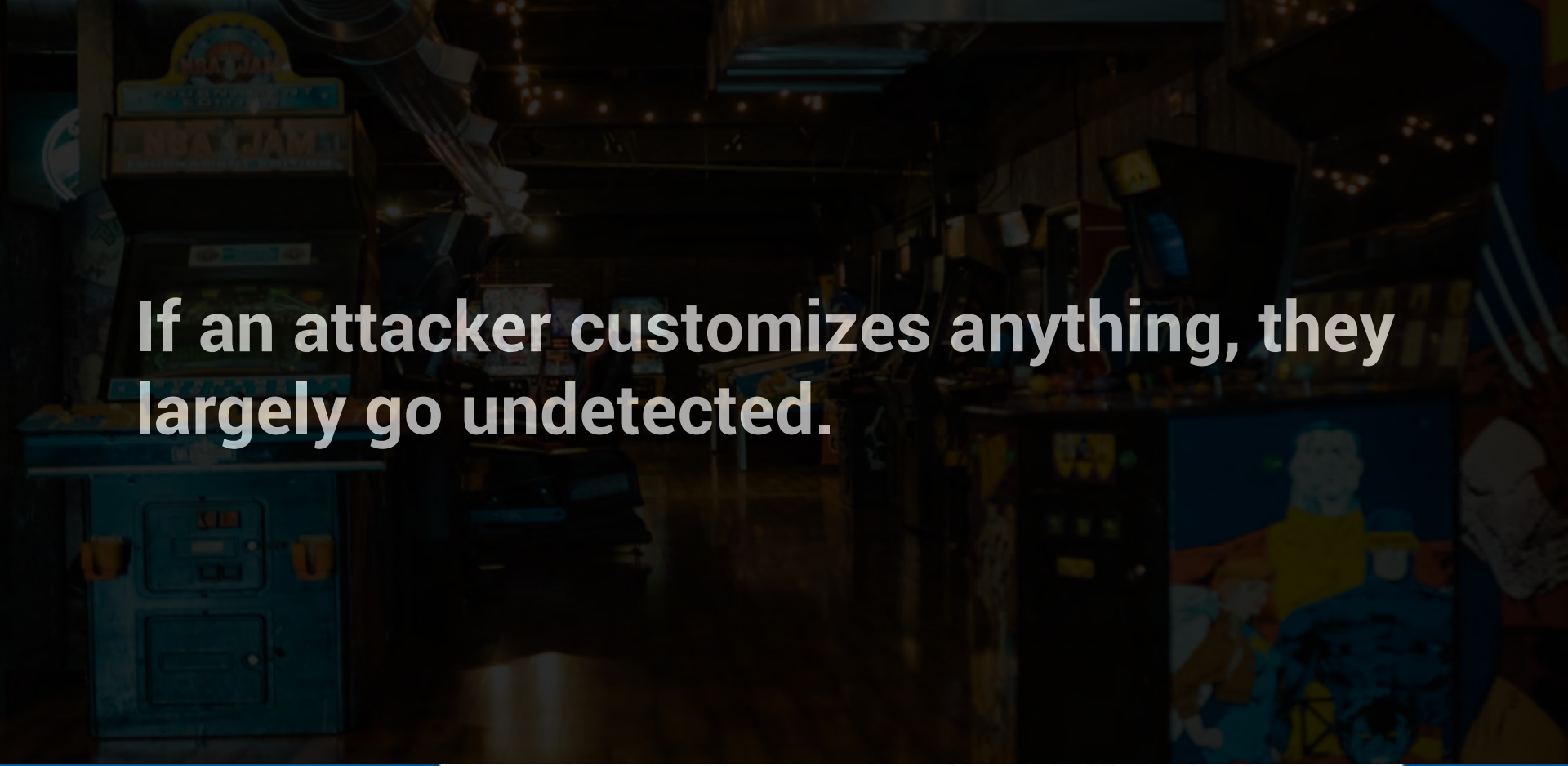
Breach Statistics

- Binary Defense analyzed over 17,323 code execution samples.
- Analysis spanned over a one year period.
- Executables still the main culprit however continual shift towards PowerShell and LOLBAS.



Breakout Timeframe

- Binary Defense analyzed over 3,912 breakout methods over a span of a year of 2018.
- Average attacker broke out of initial compromise and established foothold in under 2 hours (1.43 hours on average).
- Primary method for lateral movement was SMB/RPC through credential compromise.
- Majority of initial compromises (81%) was due to macros and attachments. Malicious websites and links in e-mail was the second highest percentage (11%), and misc. attacks (8%).

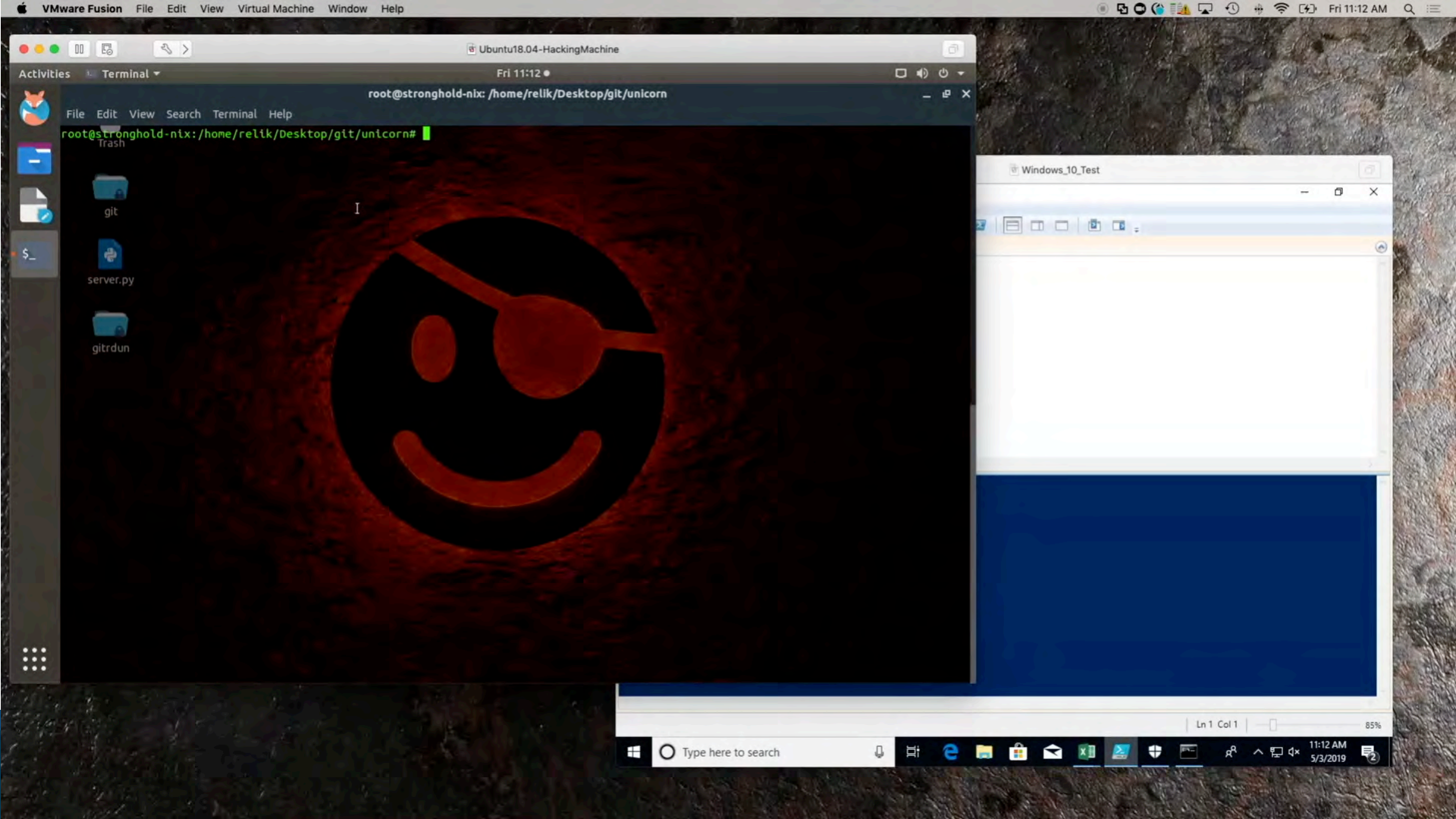

If an attacker customizes anything, they largely go undetected.


CNN Money
HACKER?

Customized Stuff

- Take a technique and modify it in anyway and you can usually circumvent all detection criteria for an organization.
- Build your own, you are sure to evade detection substantially longer than ever before.
- Leverage a technique through your own research almost ensures little to no detection.

Demonstration


VMware Fusion File Edit View Virtual Machine Window Help
Fri 11:12 AM
Ubuntu18.04-HackingMachine
Activities
Terminal
Fri 11:12
root@stronghold-nix: /home/relik/Desktop/git/unicorn
File Edit View Search Terminal Help
root@stronghold-nix:/home/relik/Desktop/git/unicorn#
Trash
git
server.py
gitrdun
Windows_10_Test
Ln 1 Col 1
85%
Type here to search
11:12 AM
5/3/2019

#5 People, Communication, Leadership

- Leadership isn't easy; I'm learning everyday.
- People are the most important security resource.
- Selling ourselves, our value, and our strategy isn't easy.
- Investments that we need to do our jobs is tough.
- Even tougher when we have no say in direction.

Closing Remarks

NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

Pushing the Security Envelope

Presented by David Kennedy CEO / TrustedSec and Binary Defense

October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | #cybersummitmn