cyrin

THE NEXT GENERATION CYBER RANGE

STOP RANSOMWARE IN ITS TRACKS

KEVIN CARDWELL
SEPTEMBER 29 2021

ARCHITECTURE
TECHNOLOGY
CORPORATION

cyrin

I’d like to welcome you today to CYRIN’s Webinar – Stop Ransomware in its Tracks! This webinar is co-hosted by CYRIN and Cyber2Labs.

My name is Paul O'Neill, head of marketing here at CYRIN.

CYRIN is a platform created by Architecture Technology Corporation, a well-known consulting and engineering firm that has been creating software solutions in the Government and Educational areas for 40+ years.

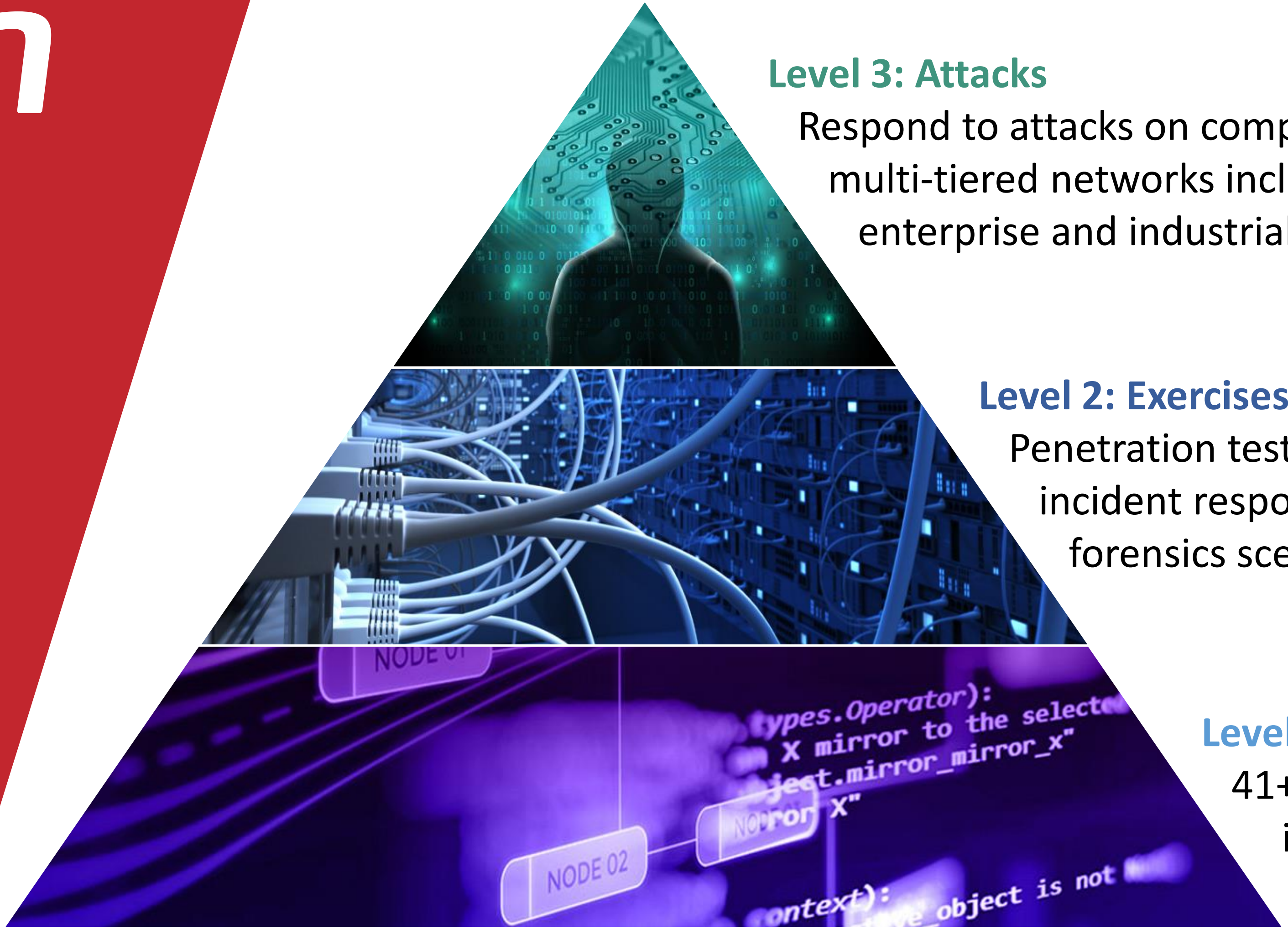
CYRIN is a next generation virtual Cyber Range. It operates in the cloud and offers students, trainers, educators and corporate cyber defenders the ability to train with real tools and real attacks to practice and improve their skills on real scenarios in a virtual sandboxed environment.

CYRIN can be accessed through most any browser, no special software required and is available 24/7, 365 days a year.

CYBER2LABS
END TO END SECURITY

cyrin

Three Levels of CYRIN Content and Service



Level 3: Attacks

Respond to attacks on complex, multi-tiered networks including enterprise and industrial control systems

Level 2: Exercises

Penetration testing and incident response / forensics scenarios

Level 1: Labs

41+ Instructional Labs in 8 Categories

New labs, exercises, and attacks released each quarter!

CYBER2LABS
END TO END SECURITY

cyrin

Introductions:

Before we get to the webinar where we have some really great content and a dynamic speaker – Kevin Cardwell, from Cyber2Labs, I'd like to introduce some members of the CYRIN team. With us today we have

Rob Joyce *- VP of Software Research and Development and technical director at CYRIN, located at our cyber division in Ithaca, NY*

Vic Thomas *- Heads up our Education Division which includes content and product management, located at Headquarters in Minneapolis*

Marshall Graham *- Director of Development and Sales*

CYBER2LABS
END TO END SECURITY

Ransomware

Today's webinar concerns a very timely topic. Ransomware is a huge global problem. According to Cybersecurity Ventures, the world-wide cost to business in 2020 was $20 billion, up from $11.5 billion a year earlier.

Yet we keep throwing money and particularly products – some estimates say over $100 billion in products in 2019 – at the problem. However, we don't seem to be solving the problem.

*A **ransomware** attack is a particularly diabolical type of attack, it not only breaches your system, but it holds it hostage until you pay the hostage taker or try and find an often time-consuming and probably more expensive workaround.*

Today Kevin Cardwell will talk about a better approach to thwart the hostage takers.

cyrin

CYBER2LABS
END TO END SECURITY

cyrin

Kevin Cardwell

is an internationally recognized cybersecurity expert who provides consulting services to companies and governments around the globe.

- *He’s an instructor, technical editor, and author for computer forensics and hacking courses*
- *He headed the team that built the U.S. Navy Network Operations and Security Center (NOSC)*
- *He created three courses on CYRIN including Cyber Skills Foundation, Essential Defense and Advanced Defense*
- *Kevin has been a frequent speaker at many well-known conferences such as Black Hat USA, Hacker Halted, ISSA and TakeDownCon*

At this point I’d like to welcome to the webinar our guest speaker Kevin Cardwell…..

CYBER2LABS
END TO END SECURITY

cyrin

Agenda

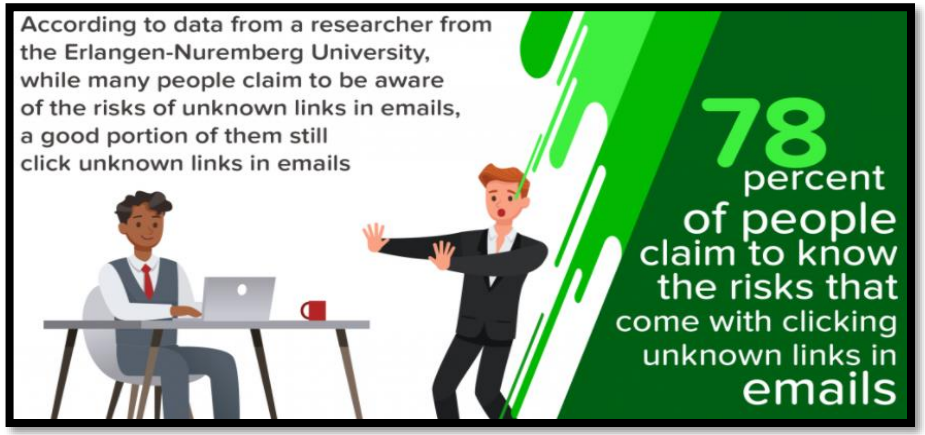
- Attack Data
- Losing the Race
- Deception Concepts
- Tools of Deception

CYBER2LABS
END TO END SECURITY

cyrin

Data Breaches

- Require users to be tricked in most cases
- We can all be tricked, even IT people



According to data from a researcher from the Erlangen-Nuremberg University, while many people claim to be aware of the risks of unknown links in emails, a good portion of them still click unknown links in emails

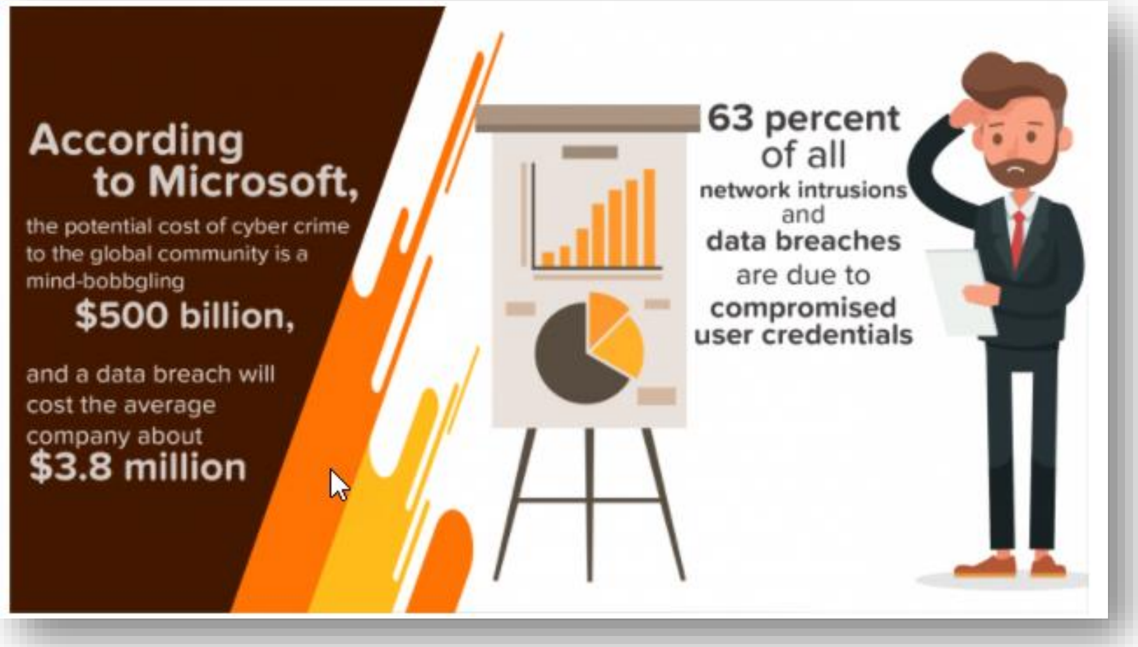
78 percent of people claim to know the risks that come with clicking unknown links in emails

https://thebestvpn.com/cyber-security-statistics-2018/

CYBER2LABS
END TO END SECURITY

Anatomy of a Breach?

- Credentials are the key
- Multi-factor authentication anyone?



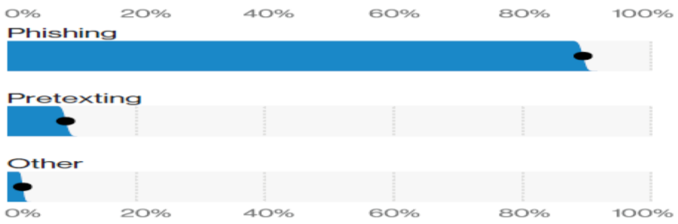
According to Microsoft, the potential cost of cyber crime to the global community is a mind-bobbgling $500 billion, and a data breach will cost the average company about $3.8 million

63 percent of all network intrusions and data breaches are due to compromised user credentials

cyrin

The Story So far

- Reality Check!
- No product will make us secure!
- Our patch system is broken
- Hardware based attacks



$27,000,000

THE AMOUNT IN U.S. DOLLARS THAT A CAR COMPANY SUBSIDIARY LOST IN 2019 TO BUSINESS EMAIL COMPROMISE

207

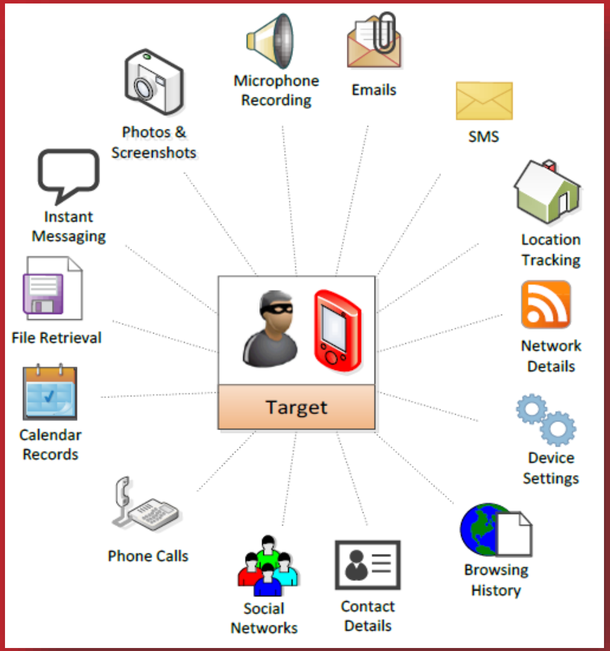
THE NUMBER OF VULNERABILITIES PATCHED IN FIVE OF THE MOST COMMON DATABASE PRODUCTS IN 2019

up from 148 in 2017

118

THE NUMBER OF DENIAL-OF-SERVICE (DOS) VULNERABILITIES THE MYSQL DEVELOPMENT PROJECT PATCHED

CYBER2LABS
END TO END SECURITY



Data and Facts

- Organized Criminal Hacker groups have advanced skills
- Assume breach
- Reality
  - Colonial Pipeline
  - SecurID source code compromise
  - Target Breach
  - WannaCry
  - Over 10 years most breaches would be blocked by:
    - fundamentals of defense

cyrin

The Race is on

- ***Criminals seem to be leading …***
- The concept has always been to keep them out
- How far has that got us?
- We need to get smarter
- Let them in!
  - Have obstacles, control the path the attacker takes
  - Nothing can keep them out 100% => we have tried that
- Once in, isolate and destroy them – Kill Chain
  - Interrupt their access

CYBER2LABS
END TO END SECURITY

cyrin

The Concept

- Unless the attacker is on the host machine directly, they are in the machine with a connection, this is our advantage
- They are residing at layer 3-4, it is our network, we control this
- In most cases the initial access is via layer 3 and by IP address
- Changing what the attacker can see
  - We can make different changes that can confuse and disrupt the attacker
    - Each disruption is a win for us on defense
    - Causes the attacker to start their methodology over again

CYBER2LABS
END TO END SECURITY

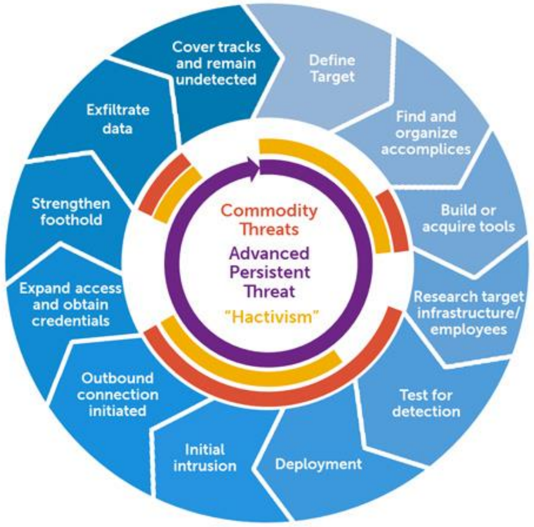
Change the advantage

- We only need ONE PACKET!
- Forever, the attackers only need one way in and now we have switched the advantage to us!

cyrin

Steps of a Successful Hack

- Surveillance
- Footprint
- Enumerate
- Identify vulnerabilities
- Exploit
- Cover Your Tracks
- Evasion


Cover tracks and remain undetected
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Commodity Threats
Advanced Persistent Threat
"Hactivism"

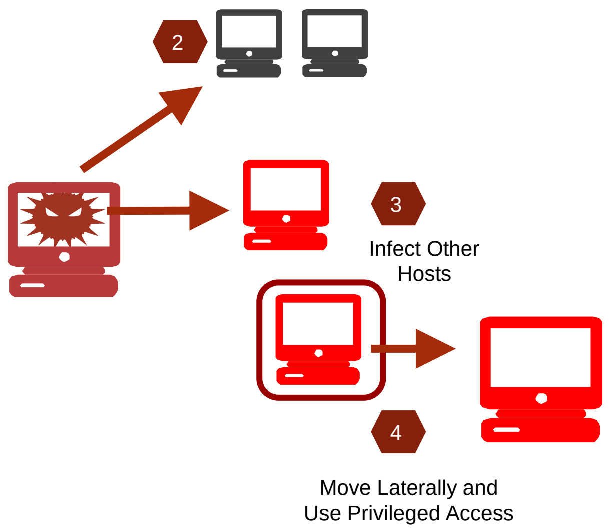
https://en.wikipedia.org/wiki/Advanced_persistent_threat

CYBER2LABS
END TO END SECURITY

Attackers Target the Whole Enterprise

Attacker Tradecraft

- Infections are a foot in the door
- Perform reconnaissance on the network
- Infect other hosts from inside and move laterally
- Use privileged hosts/accounts to access data



cyrin

Deception

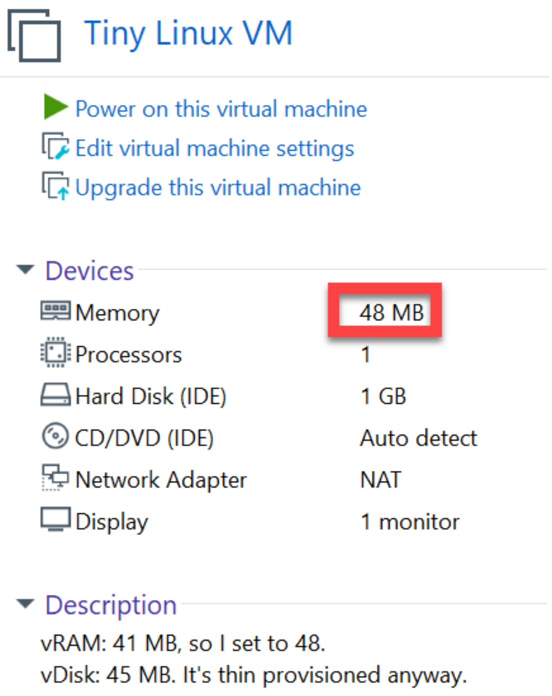
- If we break any one step of the hacking methodology steps it is a win
- Goal is to require the hacker to start the process over again
- Setup decoy machines
- Decoy ports
- Decoy services
- Decoy networks
- **Any interaction is a trigger that there is an intruder**
  - **Go to RED ALERT!**
  - **Examine the source and isolate at the switch or segment boundary**

CYBER2LABS
END TO END SECURITY

cyrin

Setting up Decoys

- Virtual
  - Use lightweight Linux distros
    - Tiny Linux
      - 48 MB of RAM
        - Nothing open by default
          - Perfect layer 3 target
- Taking existing machines and adding decoy services and ports
- Nothing should interact with it
- Setup multiple decoys on each and every segment



Tiny Linux VM

Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine

Devices

Memory	48 MB
Processors	1
Hard Disk (IDE)	1 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Display	1 monitor

Description

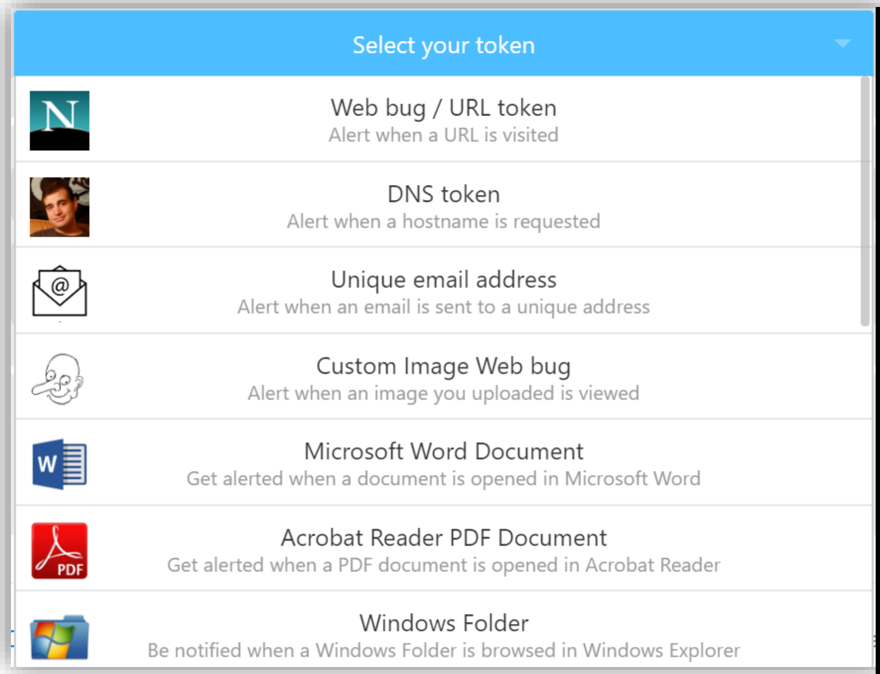
vRAM: 41 MB, so I set to 48.
vDisk: 45 MB. It's thin provisioned anyway.

CYBER2LABS
END TO END SECURITY

cyrin

Deception Options

- Any machine can be used
- Canary Tokens
  - Create custom tokens for FREE!



Select your token

Web bug / URL token
Alert when a URL is visited

DNS token
Alert when a hostname is requested

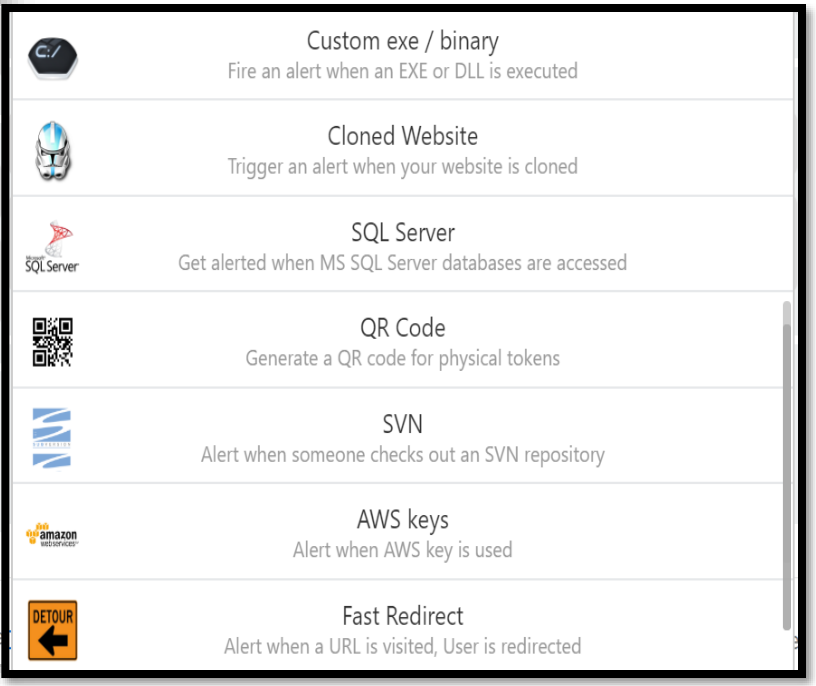
Unique email address
Alert when an email is sent to a unique address

Custom Image Web bug
Alert when an image you uploaded is viewed

Microsoft Word Document
Get alerted when a document is opened in Microsoft Word

Acrobat Reader PDF Document
Get alerted when a PDF document is opened in Acrobat Reader

Windows Folder
Be notified when a Windows Folder is browsed in Windows Explorer



Custom exe / binary
Fire an alert when an EXE or DLL is executed

Cloned Website
Trigger an alert when your website is cloned

SQL Server
Get alerted when MS SQL Server databases are accessed

QR Code
Generate a QR code for physical tokens

SVN
Alert when someone checks out an SVN repository

AWS keys
Alert when AWS key is used

Fast Redirect
Alert when a URL is visited, User is redirected

CYBER2LABS
END TO END SECURITY

Empirical Data

- It works!
- Deployed at Hacker Halted CTF and other places
- For hours no one could figure out what is real
- They had to find the doors
- Most could not without a lot of help

cyrin

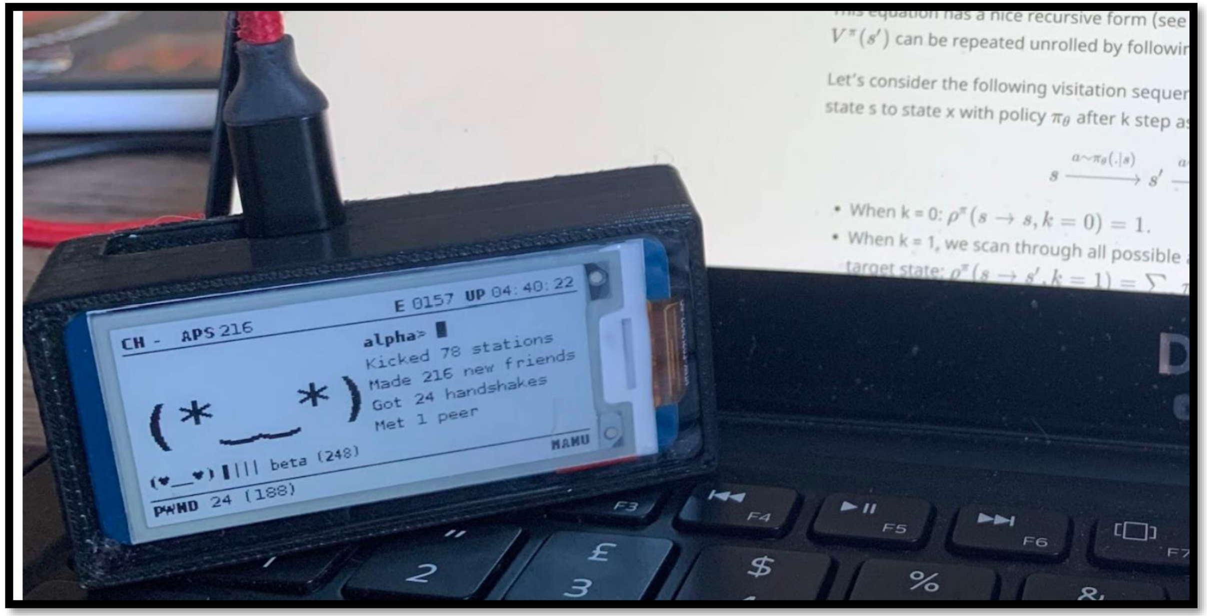
We Are in Control!

- Do not listen to the vendors etc
- We know layer 3, the hacker does not
- We control layer 3
- Deception does work!
- **One packet is all we need!**
- Deploy it on your critical segments!

CYBER2LABS
END TO END SECURITY

AI Decoys

- Deploy nodes that “learn” while in place
- Simulate the traffic that is discovered
  - Difficult to know what is real and what is false data



https://pwnagotchi.ai/

cyrin

Advanced Defense

With this course, you can be among the few who transcend the old idea of the hacker having all the fun. Take pride being the defender, form an offensive mindset to skillfully orchestrate robust and solid defenses, and reinvent popular belief by beating the hacker at his own game.

Cyber Security Skills Foundation

Gain the essential skills to build a solid security foundation. You will examine in detail the traffic that traverses the network at the packet and binary level. You will build solid knowledge on the lowest layers of the network. You will learn to master the TCP/IP protocol. You will learn essential UNIX and Linux survival skills that separate you from the many security professionals who are Windows-centric. When you finish this course you will have a solid security foundation to pursue more advanced security training.

Essential Defense Tactics

Learn the foundations of security and defending architectures from attack. You will look at the concept of "thinking like a hacker" to learn techniques to defend from the types of attacks that are commonly conducted against IT/corporate networks as well as industrial control networks. You will learn powerful methods to analyze the risks inherent in your networks. Once your foundation has been set, you will look at the best practices and recommendations for reducing attack surface. You will also learn a systematic process for intrusion and malware analysis.

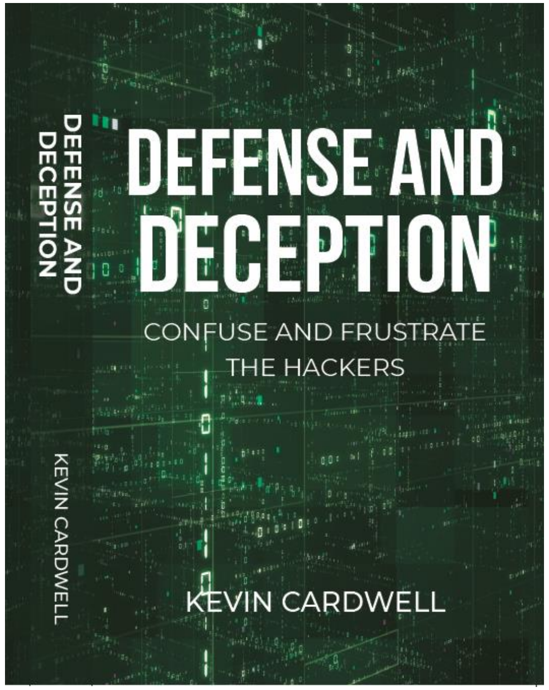
CYBER2LABS
END TO END SECURITY

cyrin

Defense and Deception

Confuse and Frustrate the Attackers

Kevin Cardwell



DEFENSE AND DECEPTION

CONFUSE AND FRUSTRATE THE HACKERS

KEVIN CARDWELL

CYBER2LABS
END TO END SECURITY

Contact US

CYRIN WEBINAR: Stop Ransomware in its Tracks!

To learn more about CYRIN, Kevin’s courses and some of the solutions you saw today.

1. Stop at our Web Site – http://www.cyrintraining.com/
2. Contact us directly at: info@cyrintraining.com
3. Call us at: 1-800-850-2170

We’re available for any questions and we offer

□ A personalized demonstration of the CYRIN platform for you and your staff and...

□ We would be delighted to allow members of your organization to try CYRIN for a free evaluation period.

□ Ask us about Kevin’s courses and **AS AN ADDED BONUS for anyone from this webinar who signs up for one of** Kevin’s courses, he will send you a signed copy of his book. (And you get a free 15-minute virtual consultation with Kevin!)

□ Thank you for your time today! And please look for your copy of the Webinar in your inbox and we look forward to hearing from you.