Cyber Threat Response

CISCO SECURITY

Simple Open Automated

cisco Security

www.cisco.com/go/security

Cyber Threat Response

Brought to you by **CISCO SECURITY**

course architects

Moses Hernandez

Ron Taylor

Katherine McNamara

Jamey Heary

William Young

John Columbus

Jeff Fanelli

Joey Muniz

Bobby Acker

Christopher Heffner

writing

Joey Muniz

art

Tariq Hassan

colors

Brian Arthur McGee

letters

Santos Vega

creative direction

Brian McGee

art direction/design

Santos Vega

editing

Andrew Akers

Smash and Grab

Chapter One

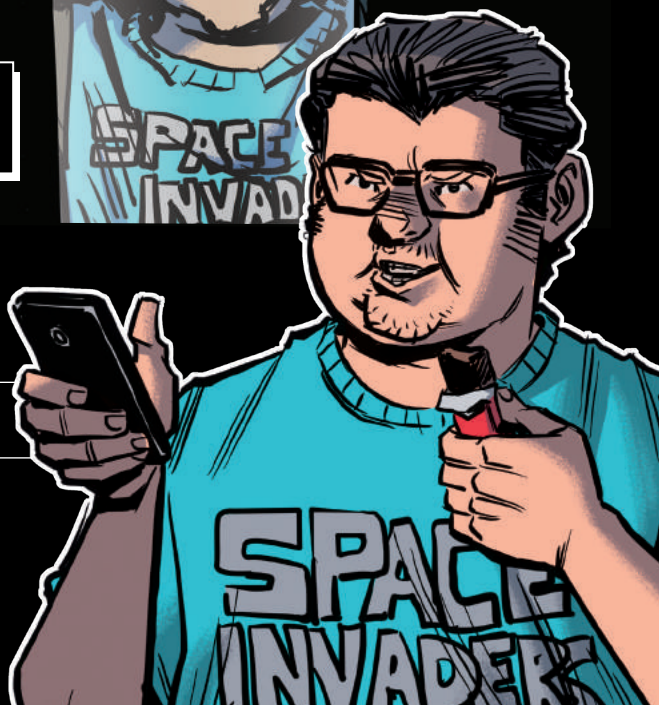

EVENING. UNKNOWN LOCATION
"I SEE YOUR HACKMDS.COM SERVERS ARE ACCESSIBLE FROM THE OUTSIDE.
"EVERYBODY HAS VULNERABILITIES.
"LET'S LOOK AT MY NOTES ON THIS TARGET."
Notes
Lacks DNS and reputation security
Standard DMZ
Skeleton IT staff
Poor patch management
Weak security defenses
Vulnerable to web attacks
Poor event monitoring
HMM
THIS WILL BE TOO EASY.
Mr. Black (alias)
Laid-off after 25 years of employment
Goal is to obtain 30 million dollars using any means available
No criminal records
No social media, false records, limited digital footprint
Proficient technologist

Mr. Orange (alias)

Known as the "Loud Jerk"

Day job unknown but has been dabbling in scripted cyber crime

Actively looking to prove himself as an elite hacker



HEY KIDS

There are lots of things to remember about **EXCELLENT** Cyber Threat Response! We know it's a lot to learn, but Cisco has you covered!

SILVER BULLET MYTH

There isn't a silver bullet for providing 100% protection against cyber crime. Sorry... we can't promise that. **NOBODY CAN!**

REDUCE RISK

You can, however, learn to reduce the risk of being compromised to an acceptable level using industry best practices for security architecture.

EDUCATE YOURSELF

The Cisco Cyber Threat Response Clinics give you hands-on experience as both **ATTACKER** and **DEFENDER** so you can better understand both sides of the cyber **CAT AND MOUSE** game.

CTR HEROES ACTIVATE!

Gone Phishing

See how easily one hacker hooks a big business

Learn how to avoid being lured in next

Watch the video story

Know your enemies

Your guide to cyber security for your business

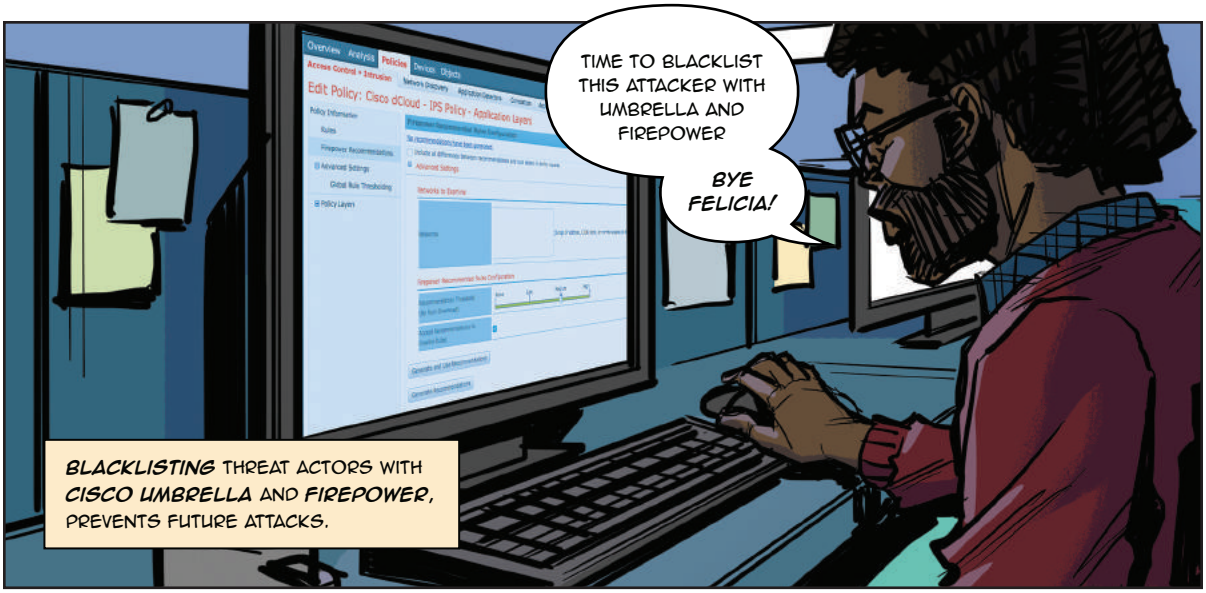
Ransomware

Malware

Read the guide

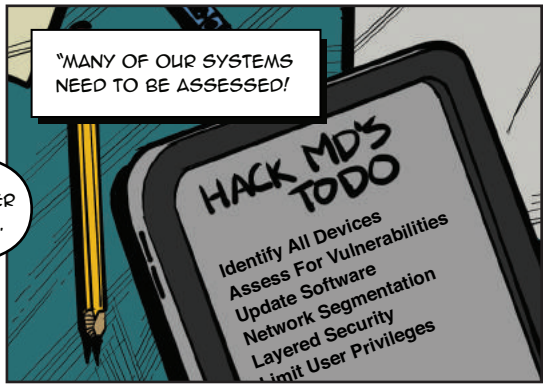
cisco


HACKMDS SECURITY OPS CENTER
FIREPOWER GROUPS VARIOUS ALERTS AS A SECURITY INCIDENT.
OUR SERVERS ARE BEING HIT BY SOMETHING
WHAT ARE THESE ALARMS?
ANY HIGH RISK INCIDENT WILL INFORM HACKMDS.
IT LOOKS LIKE SOMEBODY IS TRYING TO EXPLOIT OUR SERVERS.
GOOD THING OUR IPS IS TUNED FOR OUR ENVIRONMENT.
FIREPOWER CAN AUTO-TUNE THE IPS TO ADAPT TO NEW VULNERABILITIES WITHIN THE NETWORK.


TIME TO BLACKLIST THIS ATTACKER WITH UMBRELLA AND FIREPOWER
BYE FELICIA!
BLACKLISTING THREAT ACTORS WITH CISCO UMBRELLA AND FIREPOWER, PREVENTS FUTURE ATTACKS.


I HEARD WE WERE ATTACKED. ARE WE OKAY?


YES SIR!
CISCO FIREPOWER PREVENTED AN ATTACK AGAINST OUR SERVERS
BUT THERE ARE VULNERABILITIES THAT NEED TO BE PATCHED.
AS A MATTER OF FACT ...


"MANY OF OUR SYSTEMS NEED TO BE ASSESSED!
HACK MD'S TODO
Identify All Devices
Assess For Vulnerabilities
Update Software
Network Segmentation
Layered Security
Limit User Privileges


"WE DON'T HAVE THE MANPOWER. I'LL CALL CISCO SERVICES.
NO PROBLEM!
WE HAVE YOU COVERED
CISCO

www.xploitz.com

Infect Me Feeling Lucky

x

Don't Do It!

Exploits are everywhere!

An exploit kit is a web server designed to identify and exploit vulnerabilities in client machines. The goal is to deliver something malicious such as a backdoor or ransomware.

Exploit kits can be rented online making it easy for non-technical attackers to deliver technical attacks without understanding the details of how the attack works.

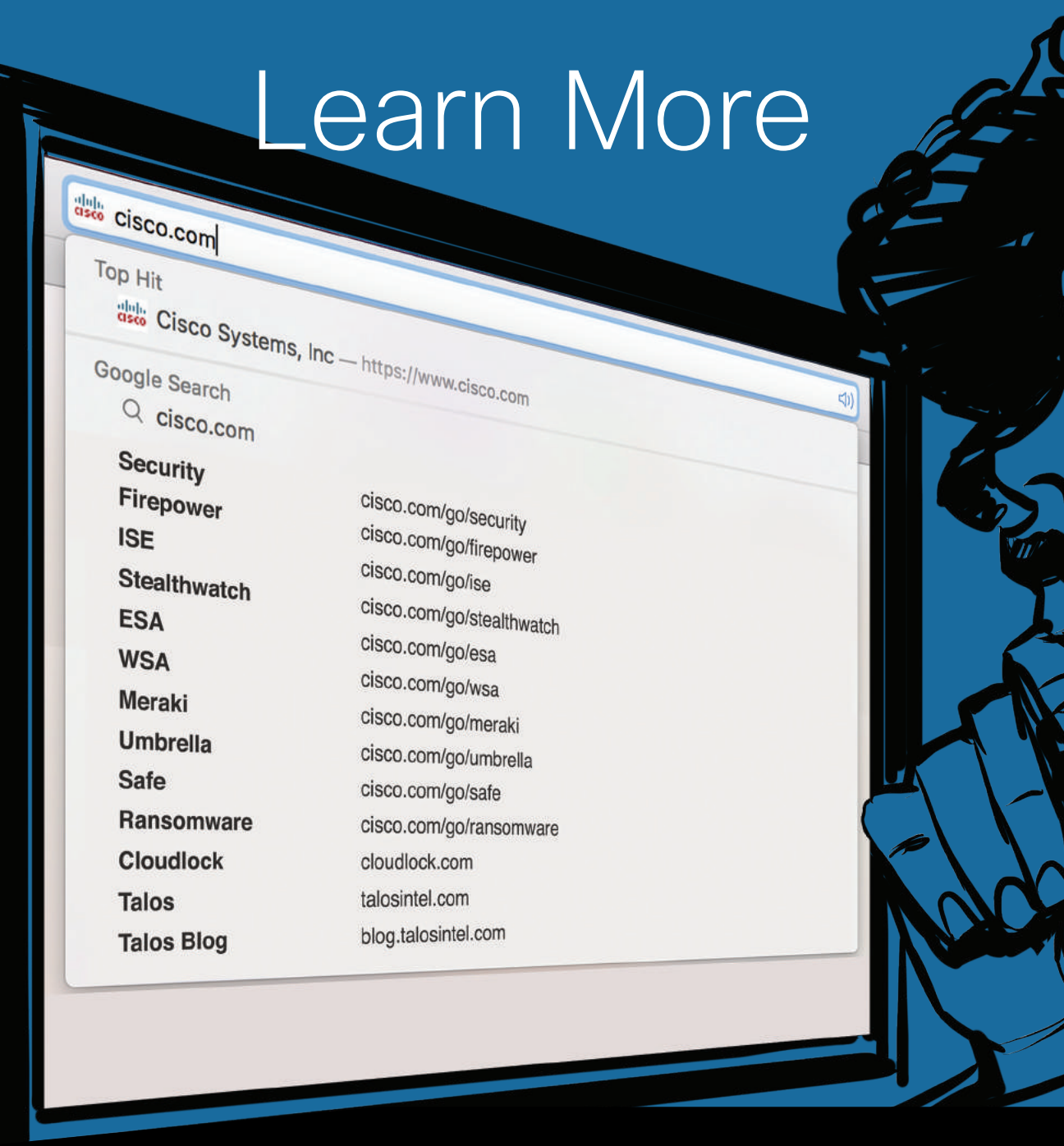
Coming Soon 2 ur CPU

Ransomware

Never stop the incident response at removing the infection, or you may experience it AGAIN!!

Identifying ransomware means an attacker was able to breach your network and deliver malicious software. **Best practice is to identify and remediate infected machines, harden the network against the attack method used, and blacklist any sources linked to the original attack!**

Learn More



We hope you enjoyed the Cisco Cyber Threat Response Clinic!

Make sure to come back and complete any modules you didn't have a chance to work on and check back for more future modules!

Cisco Security

Product Suite

Firepower
URL, IPS, and Breach security

Cisco Umbrella
DNS Security and forensics

ESA
Email security for cloud and on-prem

ISE
Access control and security policy management

Meraki
Cloud managed security, network and collaboration

AMP
Advanced breach detection for endpoint and network

VPN
Encrypted communication

Stealthwatch
Netflow anomaly monitoring and breach detection

Cisco Cloudlock
Cloud application security

Threatgrid
Threat analytics, detection and prevention

Talos
Security research and threat intelligence

WSA
Secure proxy, content control and security

Physical · Virtual · Cloud