

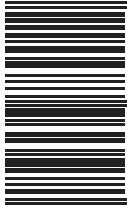


\$FREEus

RATED S SECURITY



10001010010



0 100001101010

Cyber Threat Response
CISCO SECURITY



Simple



Open



Automated



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

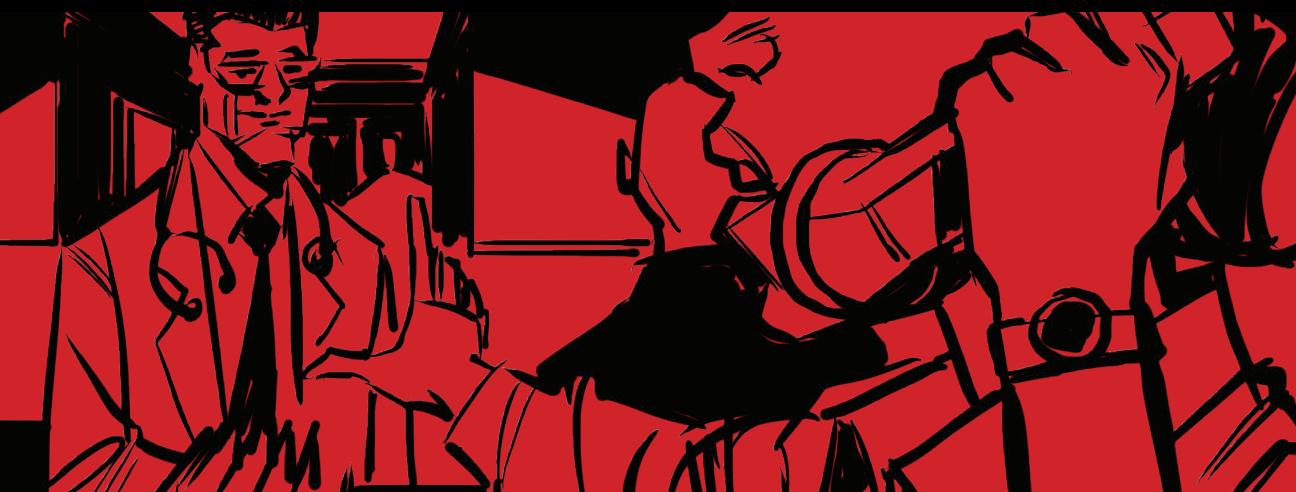
Santos Vega

editing

Andrew Akers

Copyright © 2017 Cisco and/or its affiliates. All rights reserved.





Compromised Laptop

Chapter Four

THE NEXT MORNING

I CAN CREATE A FAKE FANTASY STATS PAGE AND EMAIL HIM A LINK TO HIS PERSONAL ACCOUNT.

"DR. HOWSER LIKES FANTASY FOOTBALL ACCORDING TO FACEBOOK."

"IT WILL DROP MALWARE ONTO HIS SYSTEMS WHEN HE ACCESSES THE WEBSITE FROM HOME."

DR. HOWSER

"DR. HOWSER WILL GO BACK TO WORK AND CONNECT HIS INFECTED SYSTEM TO THE HACKMDs NETWORK."

GIVING ME INSIDE ACCESS.

"LET'S LOOK AT MY NOTES ON THIS TARGET."

Notes

People will click anything without thinking about it

Limited host security software that is based on signatures

HackMDs not responsible for user's home network

Compromised hosts can provide internal access for outsiders

Social engineering is extremely effective



EMAIL SENT
LET'S SEE IF DR. HOWSER WILL ACCESS MY FAKE WEBSITE.

"DR. HOWSER WILL CONNECT HIS LAPTOP OVER VPN WHILE AWAY FROM THE OFFICE."



PROVEN FOOTBALL STATS?
MY TEAM IS GETTING KILLED.

CAN'T HURT TO SEE WHAT THEY SAY

MALICIOUS WEBSITES WILL SCAN A VICTIM'S SYSTEMS FOR WEAKNESSES SUCH AS FLASH AND JAVA VULNERABILITIES.



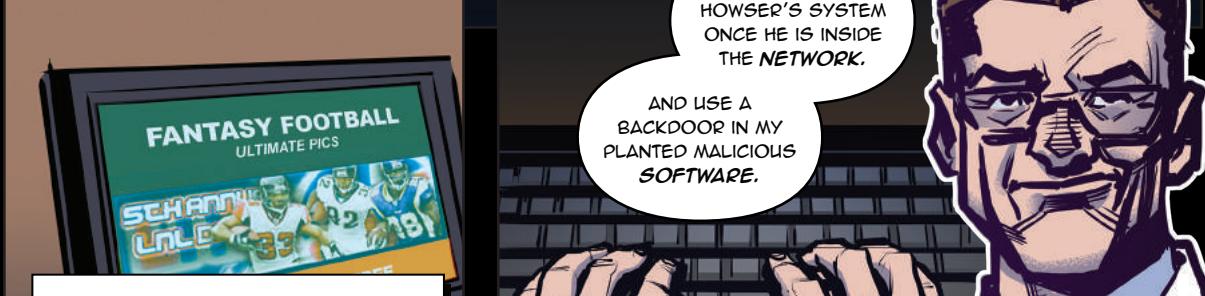
I'LL EXPLOIT THAT TO PLACE MY MALWARE ON HIS SYSTEM.

DR. HOWSER'S JAVA IS OUT OF DATE.



I'LL ACCESS DR. HOWSER'S SYSTEM ONCE HE IS INSIDE THE NETWORK.

AND USE A BACKDOOR IN MY PLANTED MALICIOUS SOFTWARE.



"I WILL OWN HACKMOS THROUGH HIS COMPUTER USING HIS SYSTEM AS MY UNKNOWN INSIDE ATTACKER."

"I'LL CALL HIM MR. RED."

Mr. Red (alias)

This could be anybody within the organization knowingly or unaware

Example: Breached system is used remotely by a hacker to access internal sources

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!

There isn't a silver bullet for providing 100% protection against cyber crime. Sorry... we can't promise that.

NOBODY CAN!

REDUCE RISK

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!



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

EDUCATE YOURSELF

Your Ad Here

HACKMD'S SECURITY OPS CENTER.

INTERESTING

FIREPOWER
SAYS ONE OF
OUR USERS IS
COMPROMISED.

ISE EVALUATES DEVICES BEFORE THEY
ARE PERMITTED ACCESS AND SHARES
CONTEXT WITH OTHER TECHNOLOGIES.

THIS IS HOW ISE KNOWS AN IP ADDRESS
IS LINKED TO DR. HOWSER'S LAPTOP.

HI BOSS,

CAN YOU SWING
BY MY OFFICE?
WE HAVE A
PROBLEM.

ISE USES TRAFFIC SEEN FROM DEVICES VS
MAC ADDRESS TO DETERMINE WHAT THEY ARE.

FIREPOWER CAN ALERT ISE TO QUARANTINE
ANY DEVICE SEEN AS COMPROMISED.

THE FIREPOWER AND ISE COMBINATION
CAN PROVIDE 24/7 SECURITY MONITORING ...

AND ENFORCEMENT OF POLICY ON ALL
DEVICES ACCESSING THE NETWORK.

THAT'S DR. HOWSER'S
PERSONAL WINDOWS
LAPTOP CAUSING
THESE ISSUES

DR HOWSER'S
LAPTOP HAS BEEN
OWNED AND
VPNED INTO OUR
NETWORK.

\$#@%!!

HOW DID
THIS HAPPEN?

SOMEBODY
GET HIM OFF THE
NETWORK!

NO NEED TO
REMOVE HIM.
THE NETWORK
SAW THE ISSUE.

IT AUTO
QUARANTINED
HIM.

SEEMS LIKE DR.
HOWSER'S SYSTEM
IS BEING USED AS
AN ATTACKER'S
PROXY OVER VPN.

WOW!
MY NETWORK IS A
SECURITY BOUNCER
AND ENFORCER.

STEP AWAY
FROM THE
NETWORK SIR.

SECURITY

www.xploit.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

A stylized illustration of a hand holding a magnifying glass, focusing on a computer monitor. The monitor displays a search results page for "cisco.com". The top result is "Top Hit: Cisco Systems, Inc — https://www.cisco.com". Below the search bar, there is a list of links corresponding to various Cisco products and services, each with its respective URL. The background is a solid blue color.

Link	URL
Google Search	cisco.com
Security	cisco.com/go/security
Firepower	cisco.com/go/firepower
ISE	cisco.com/go/ise
Stealthwatch	cisco.com/go/stealthwatch
ESA	cisco.com/go/esa
WSA	cisco.com/go/wsa
Meraki	cisco.com/go/meraki
Umbrella	cisco.com/go/umbrella
Safe	cisco.com/go/safe
Ransomware	cisco.com/go/ransomware
Cloudlock	cloudlock.com
Talos	talosintel.com
Talos Blog	blog.talosintel.com

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



VPN

Encrypted communication



Cisco Umbrella

DNS Security and forensics



Stealthwatch

Netflow anomaly monitoring
and breach detection



ESA

Email security for cloud and
on-prem



Cisco Cloudlock

Cloud application security



ISE

Access control and security
policy management



Threatgrid

Threat analytics, detection
and prevention



Meraki

Cloud managed security,
network and collaboration



Talos

Security research and threat
intelligence



AMP

Advanced breach detection
for endpoint and network



WSA

Secure proxy, content control
and security

Physical · Virtual · Cloud