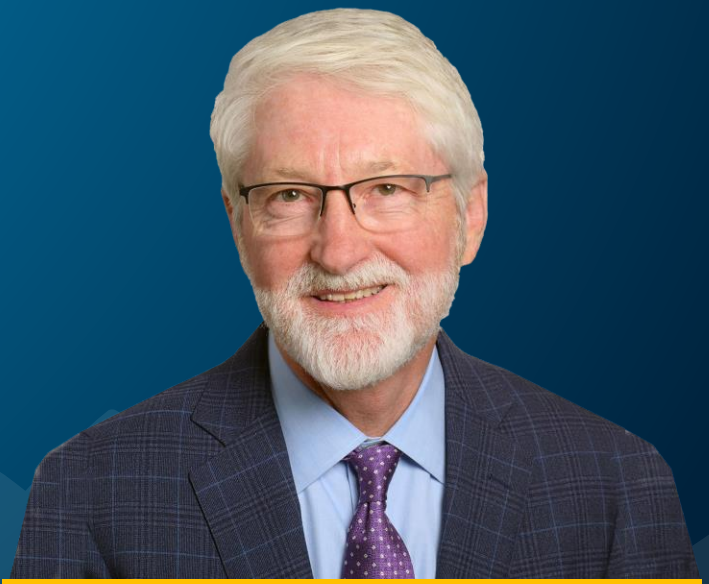
CyberCenter:
Post-Game Analysis

Steve Petrovich



Steve Hinkle

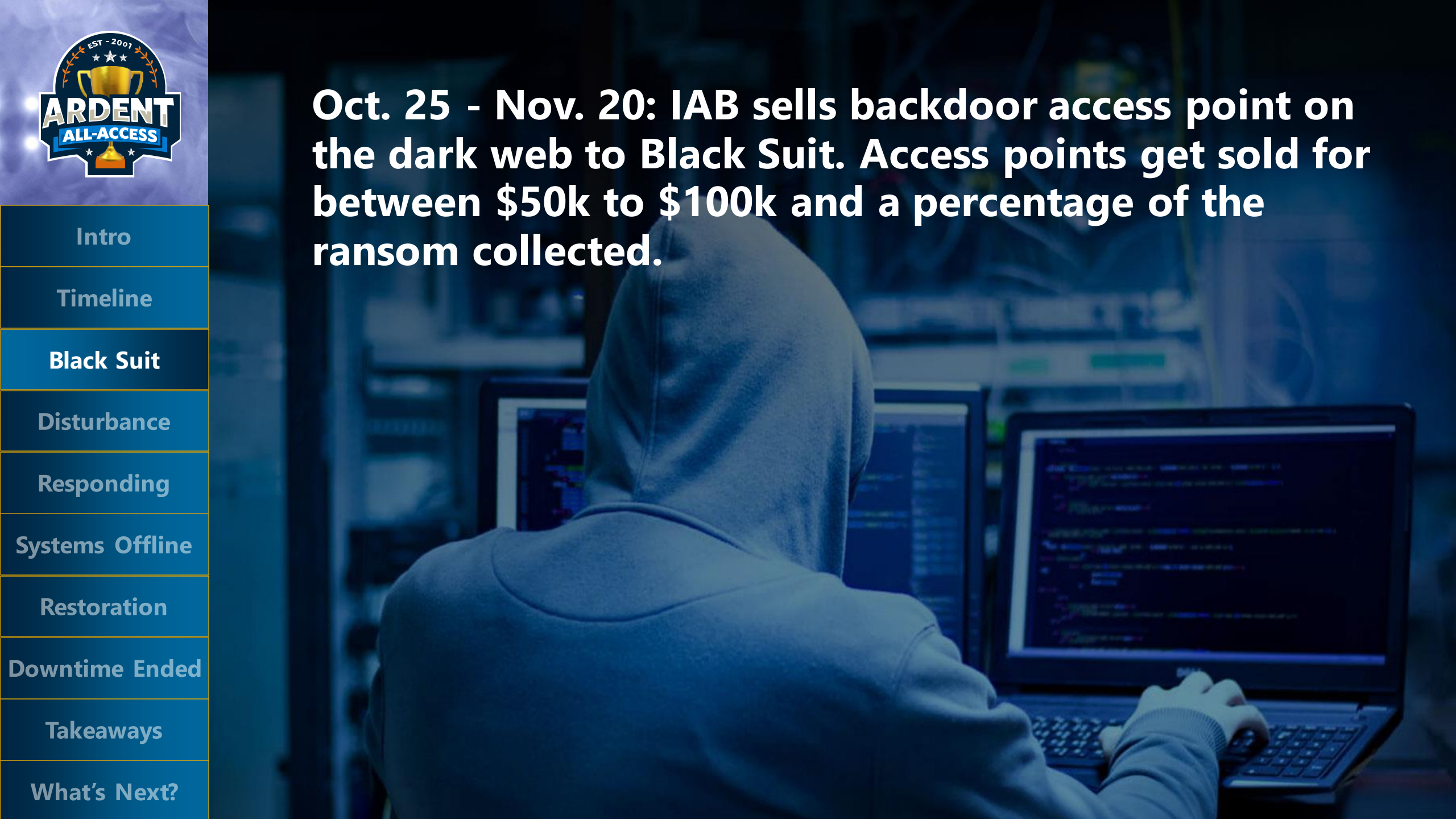
Anika Gardenhire

A look into the recent cyber event from initial contact to Epic Go live.

- We were "attacked" by two entities in separate waves
  - Initial Access Broker and Black Suit cybercriminal hacker group
    - An initial access broker places executable files on legitimate websites and waits for unsuspecting travelers to download its corrupted materials to create access points to otherwise secure systems. The IAB in our scenario was not trying to access our system.
    - Black Suit: a cyber-criminal group whose business is to infiltrate secure systems, encrypt hardware, exfiltrate data and cause as much chaos as they can before being paid a ransom to return things to normal.

What we know now – timeline of events

- Oct. 25: Patient Zero traversed the internet and fell victim to a Search Engine Optimization Poisoning event by being led to a corrupted site.
  - The downloaded file was able to create an access point that bridged into our systems. That access point was then sold on the dark web to the hacker group, Black Suit.
  - When the PDF opens, the gootloader file launched and created back door, hidden access into Ardent network.



Oct. 25 - Nov. 20: IAB sells backdoor access point on the dark web to Black Suit. Access points get sold for between $50k to $100k and a percentage of the ransom collected.

Oct. 25 - Nov. 20: IAB sells backdoor access point on the dark web to Black Suit. Access points get sold for between $50k to $100k and a percentage of the ransom collected.

- Nov 20: Black Suit utilizes the back door created by the IAB and enters our secure system through a single hospital domain.
- They utilize a Gootloader software as well as other Microsoft applications to begin exploration of our system and "hide in plain sight"
- They were well prepared - so were we.

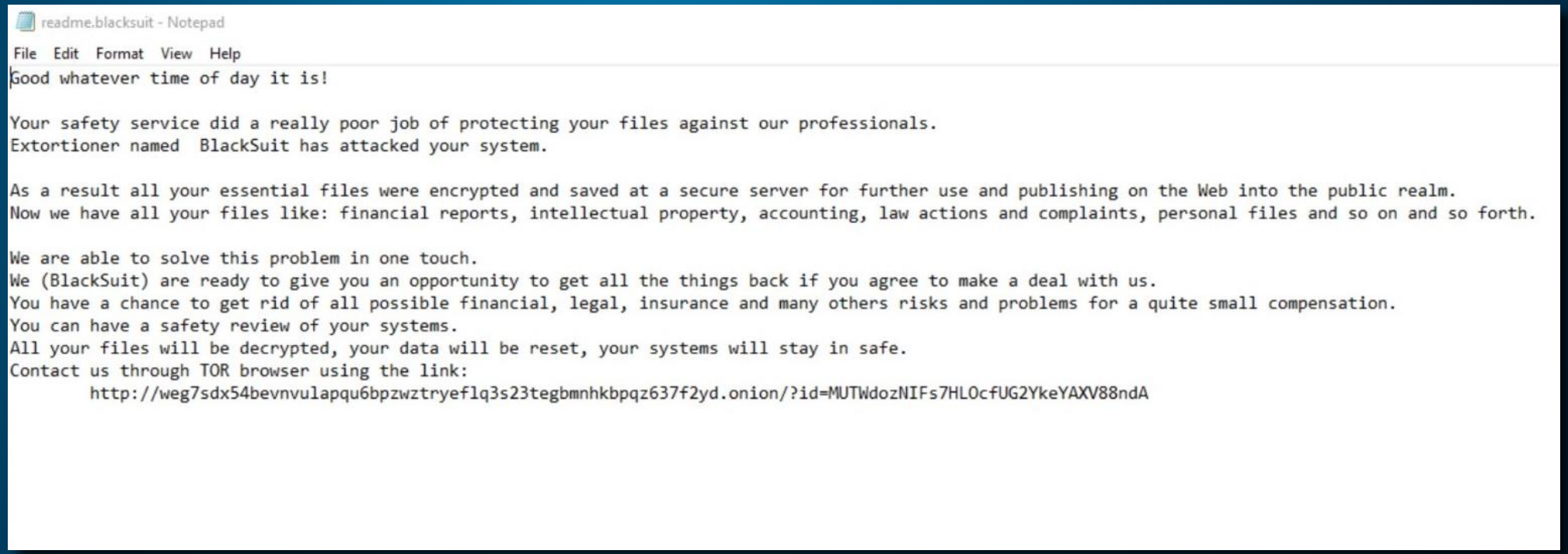
Nov. 20: Government noticed disturbance in internet activity.

- CISA, FBI and a third party notice significantly increased and unusual activity from our domain, but because "a unique attack vector utilized" they are unable to identify the exact nature of the activity.
- It was noted that more energy than normal was being utilized and more transmissions were occurring.

Nov. 20-23: Ardent security personnel and retained third party security vendor institute response and recovery efforts.

- Engineers work to identify, contain and expunge threat from the system. Unique attack vector and activity make it difficult to track and identify true nature of the threat.
- Third-party vendor engages additional resources in effort to contain spread of Trojan malware and carbon-based lifeform accessing our systems.

Nov. 23: First ransomware message seen on PACS monitor in Albuquerque – confirming ransomware attack.



readme.blacksuit - Notepad

File Edit Format View Help

Good whatever time of day it is!

Your safety service did a really poor job of protecting your files against our professionals.
Extortioner named BlackSuit has attacked your system.

As a result all your essential files were encrypted and saved at a secure server for further use and publishing on the Web into the public realm.
Now we have all your files like: financial reports, intellectual property, accounting, law actions and complaints, personal files and so on and so forth.

We are able to solve this problem in one touch.
We (BlackSuit) are ready to give you an opportunity to get all the things back if you agree to make a deal with us.
You have a chance to get rid of all possible financial, legal, insurance and many others risks and problems for a quite small compensation.
You can have a safety review of your systems.
All your files will be decrypted, your data will be reset, your systems will stay in safe.
Contact us through TOR browser using the link:
http://weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd.onion/?id=MUTWdozNIFs7HLOcfUG2YkeYAXV88ndA

Nov. 23: First ransomware message seen on PACS monitor in Albuquerque – confirming ransomware attack.

- By this time, threat had laterally moved among domains, gained access to the Ardent domain, spread to all system domains and hospitals.
- Notices begin appearing across network
- Multiple systems affected and clinical operations reduced
- Data exfiltrated and encryptions begin
- Hospitals go on divert
- Ardent Command Center and secure communications channels created
- Additional resources retained and plans deployed for downtime procedures

ANIKA GARDENHIRE

Chief Digital Information Officer

CyberCenter:
Special Guest

Nov. 24: Ardent takes all systems down

- "Unplugging the internet" – not as simple as a switch
- Initiated full downtime procedures – Epic read-only
- Veteran team members step up to teach colleagues how to operate on paper only.
- Accelerate efforts to contain Trojan horse malware from replicating.
- Contact threat actor and move to private dark web chat. FBI states actors' response is unusual.

Nov. 25 – Dec. 5: Intense defensive maneuvers

Nov. 25 – Dec. 5: Intense defensive maneuvers

- Once internet is down, Ardent switches to offense:
  - Rebuild domain controllers
  - Insulate active directories
  - Mandate password change
  - Cocoon servers
  - Protect clean restore points for data backup
  - Accelerate deployment of additional anti-virus software
  - Enhance communications with regulatory and law enforcement agencies
  - Execute communications plan for all stakeholders and public

Nov. 25 – Dec. 5: Trojan horse contained: work begins restoring infrastructure

- Engineers rebuilding domain controllers, servers and isolating corrupted end points. Push out new anti-virus routines.
- Begin password reset for all users, devices and service accounts.
- Hospitals change divert status based on capabilities and capacity, as they stabilize and recover clinical operations.
- Prioritization of systems to restore once restoration point established: Epic, critical clinical systems, Ensemble connection, financial connections.

Dec. 5: Epic restored ending full downtime procedures

- The largest Epic go-live ever, as teams continue work to bring other systems back online.
- Communication and transmission to vendors opens.
- Clean and secure environment verified.
- Restoration assessment of more than 6,000 servers, 400 applications and 180 domain controllers.

ANIKA GARDENHIRE

Chief Digital Information Officer

CyberCenter:
Special Guest

Takeaways

- Our team is very resilient and adaptable – remarkable.
- Training for full hospital downtime procedures is worthwhile.
  - Using non-Wi-Fi based systems for communications and sharing information: runners, walkie talkies, paper notices, etc.
  - Creating closed circuit intra-hospital monitoring and data sharing:
    - Re-training staff to use paper, non-internet based IV machines, buying printers, paper, toner, non-Ardent network Wi-Fi cellular based systems

Where we are now and what's next

- Mailed notices to all 40,000 impacted individuals, and notified several state attorneys general.
- Working with regulatory agencies on reporting issues.
- Compiling insurance claim, while addressing class action claims.
- Updating security protocols and completing full restoration.


EST - 2001
ARDENT
ALL-ACCESS