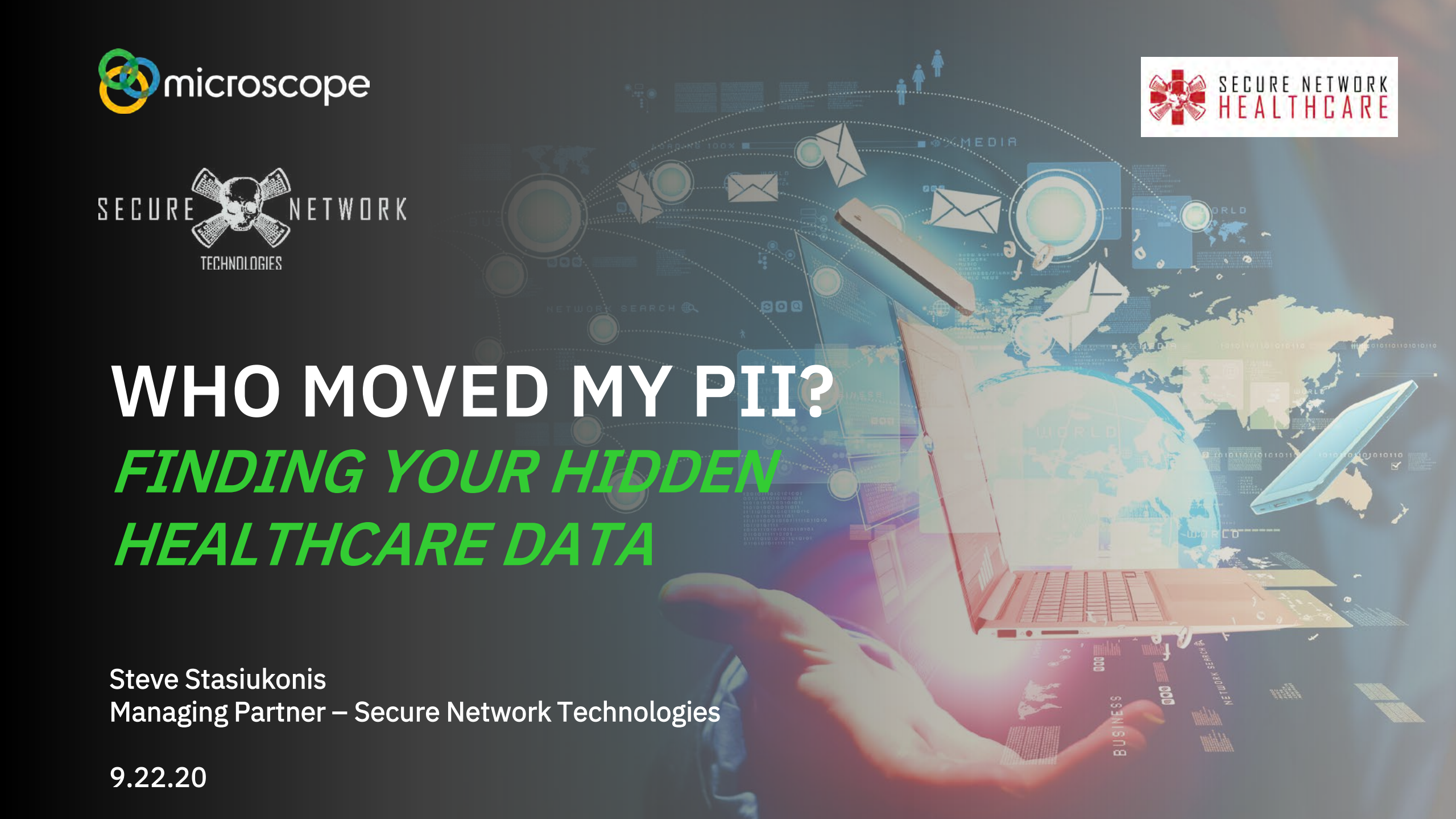


WHO MOVED MY PII?

FINDING YOUR HIDDEN HEALTHCARE DATA

Steve Stasiukonis
Managing Partner – Secure Network Technologies

9.22.20

DISCLAIMER

The material in this presentation, and presented during this webcast, is designed for, and intended to serve as an aid to, continuing professional education. Due to the certainty of continuous current developments in the healthcare industry, these materials are not appropriate to serve as the sole authority for any opinion or position relating to the subject matter. They must be supplemented with the authoritative source. Before making any decisions, or taking any action, you should consult the underlying authoritative guidance and if necessary, a qualified professional advisor.

The presenters, Secure Network Technologies and microscope HC LLC shall not be held responsible for any loss sustained by any person who relies on this material or presentation made by the presenters.

Copyright is not claimed in any material secured from official US government sources.

microscope

HOW TO GET CPE

1. At some point during the webinar, please be sure to type a message or question into the chat OR question box.
2. Be sure to complete the survey (evaluation) at the end of the webinar.

*If there is an issue with your chat box/question box or if your evaluation does not populate, please email Jackie Al-Nwiran @ jackieA@microscopeHC.com to receive credit.

CPE Certificates will be emailed out next week.

*Questions: There will be time allotted at the end of the presentation for a brief Q&A. You can type your questions throughout the presentation into the question box and they will be answered in the order in which they were received.

* This presentation will be available in PDF format by request.

microscope

TODAY'S PRESENTER

Steve Stasiukonis

Managing Partner – Secure Network Technologies

Steve focuses on Penetration Testing, Information Security Risk Assessments, Incident Response and Digital Investigations. Steve has worked in the field of Information Security since 1997. As a part of that experience, Steve is an expert in Social Engineering and has demonstrated actual social engineering efforts involving pretexting, phishing and physically compromising financial institutions, data centers and other secure facilities. Steve has contributed to Darkreading and Information Week since 2006.

SECURE NETWORK

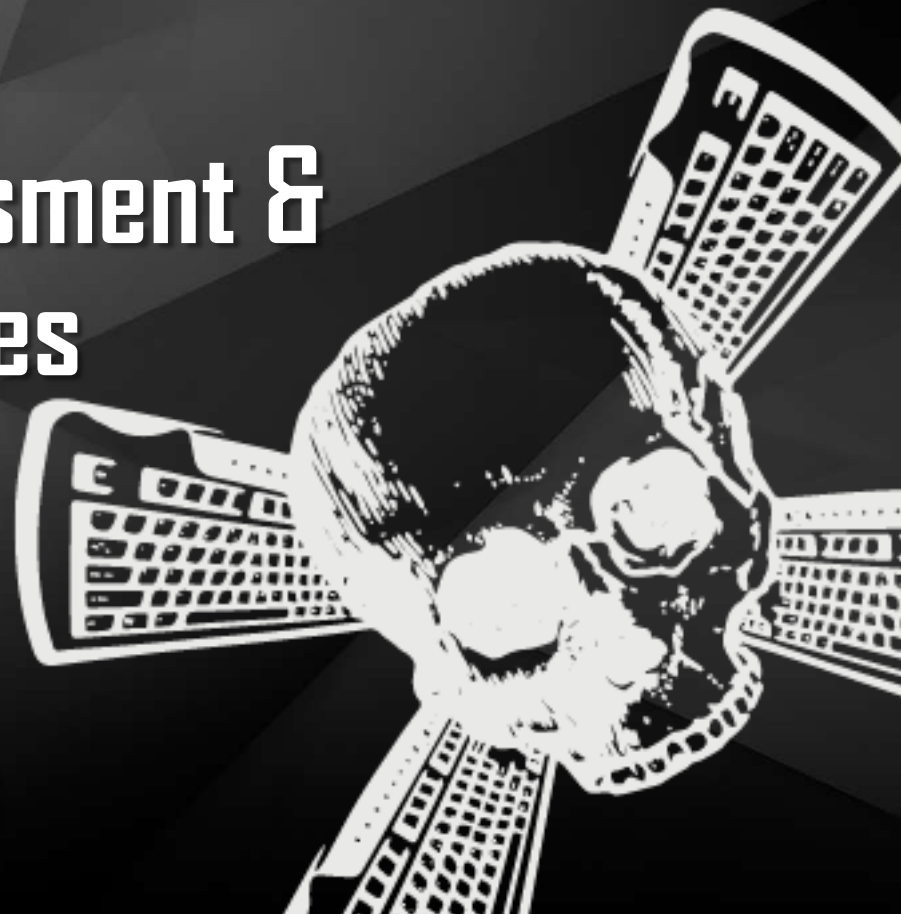
TECHNOLOGIES

ABOUT SECURE NETWORK

ESTABLISHED IN 1997

Perform Security Assessment & Penetration Services

Perform Incident Response Services



WHO MOVED MY PII
"PERSONAL IDENTIFIABLE INFORMATION"

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for deanonymizing previously anonymous data can be considered PII

HOW HACKERS LOCATE PII?

2020 HEALTHCARE DATA DISASTERS

AVEANNA HEALTHCARE: 166,077 PATIENTS

POORLY MANAGED SYSTEMS EXFILTRADED DATA

PIH HEALTH: 199,548 PATIENTS

PROTECTED SYSTEM VIA COMPROMISED EMAIL ACCOUNTS

MAGELLAN HEALTH: 365,000 PATIENTS

RANSOMWARE & EXFILTRATION OF DATA

BENEFIT RECOVERY SPECIALISTS: 274,837 PATIENTS

MALWARE EXFILTRATION

AMBRY GENETICS: 232,772 PATIENTS

COMPROMISED EMAIL ACCOUNTS

FLORIDA ORTHOPAEDIC INSTITUTE: 640,000 PATIENTS

RANSOMWARE & EXTORTION

BJC HEALTH SYSTEM: 287,876 PATIENTS

COMPROMISED EMAIL

ELITE EMERGENCY PHYSICIANS (FORMERLY KNOWN AS ELKHART EMERGENCY PHYSICIANS): 550,000 PATIENTS

INCOMPETENT DATA DESTRUCTION VENDOR

HEALTH SHARE OF OREGON: 654,000 PATIENTS

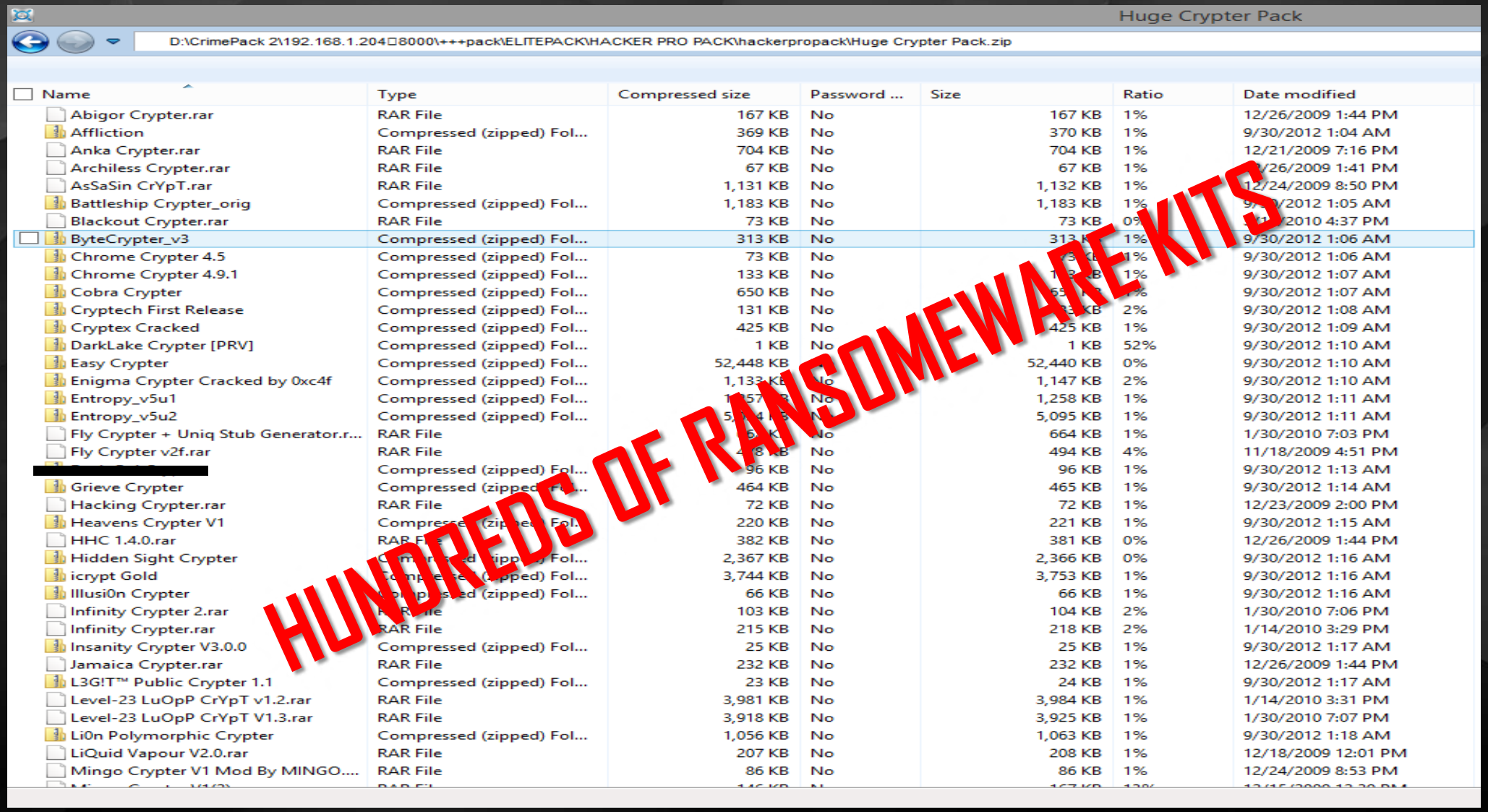
LOST LAPTOP

BST & CO. CPAS: 170,000 PATIENTS

RANSOMWARE & EXTORTION

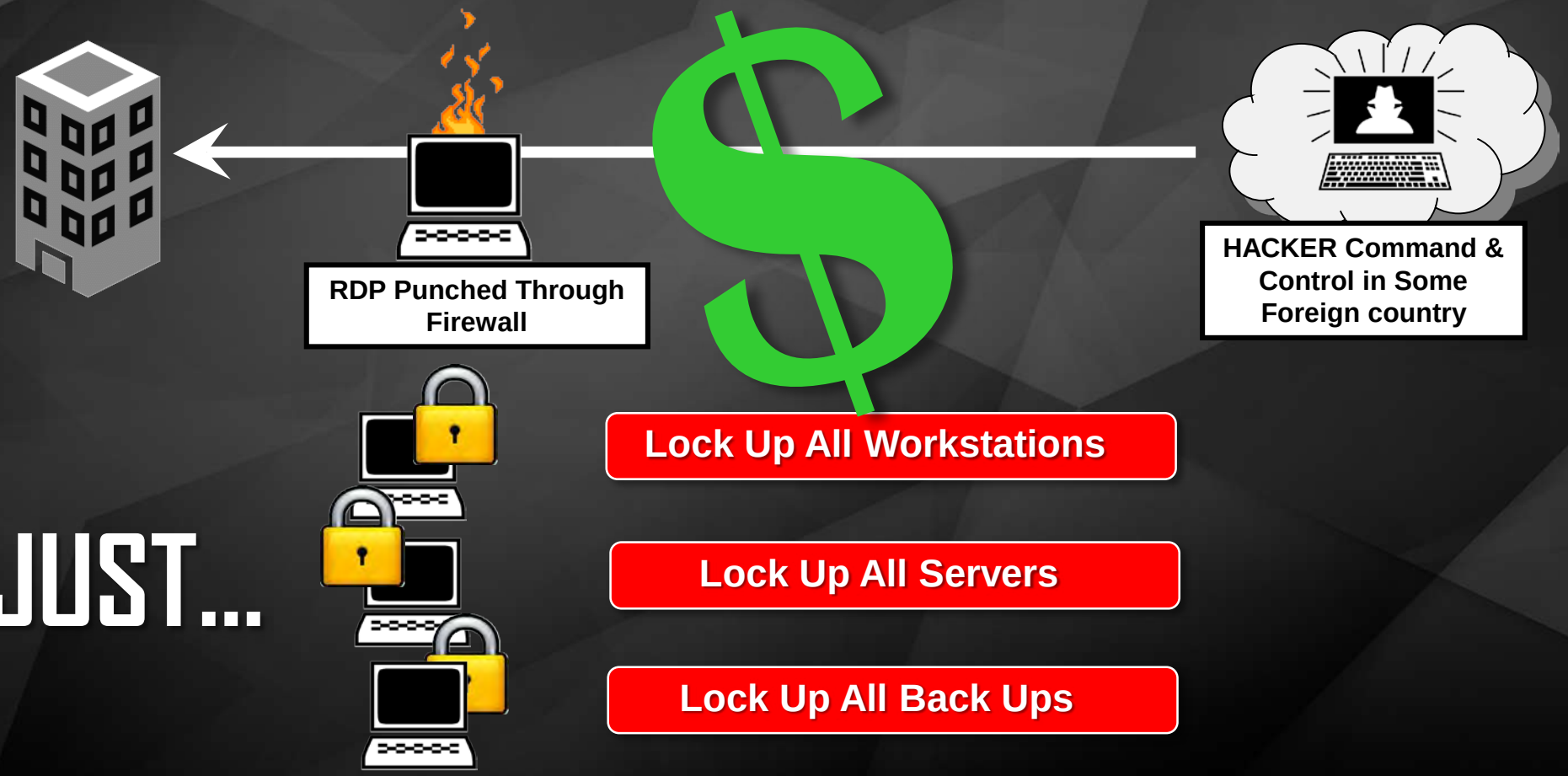
WHY GO AFTER HEALTHCARE PII?

HACKERS LIKE LOCKING UP DATA



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
Abigor Crypter.rar	RAR File	167 KB	No	167 KB	1%	12/26/2009 1:44 PM
Affliction	Compressed (zipped) Fol...	369 KB	No	370 KB	1%	9/30/2012 1:04 AM
Anka Crypter.rar	RAR File	704 KB	No	704 KB	1%	12/21/2009 7:16 PM
Archiless Crypter.rar	RAR File	67 KB	No	67 KB	1%	/26/2009 1:41 PM
AsSaSin CrYpT.rar	RAR File	1,131 KB	No	1,132 KB	1%	12/24/2009 8:50 PM
Battleship Crypter_orig	Compressed (zipped) Fol...	1,183 KB	No	1,183 KB	1%	/2012 1:05 AM
Blackout Crypter.rar	RAR File	73 KB	No	73 KB	0%	/2010 4:37 PM
ByteCrypter_v3	Compressed (zipped) Fol...	313 KB	No	313 KB	1%	9/30/2012 1:06 AM
Chrome Crypter 4.5	Compressed (zipped) Fol...	73 KB	No	73 KB	1%	9/30/2012 1:06 AM
Chrome Crypter 4.9.1	Compressed (zipped) Fol...	133 KB	No	133 KB	1%	9/30/2012 1:07 AM
Cobra Crypter	Compressed (zipped) Fol...	650 KB	No	651 KB	1%	9/30/2012 1:07 AM
Cryptech First Release	Compressed (zipped) Fol...	131 KB	No	133 KB	2%	9/30/2012 1:08 AM
Cryptex Cracked	Compressed (zipped) Fol...	425 KB	No	425 KB	1%	9/30/2012 1:09 AM
DarkLake Crypter [PRV]	Compressed (zipped) Fol...	1 KB	No	1 KB	52%	9/30/2012 1:10 AM
Easy Crypter	Compressed (zipped) Fol...	52,448 KB	No	52,440 KB	0%	9/30/2012 1:10 AM
Enigma Crypter Cracked by 0xc4f	Compressed (zipped) Fol...	1,133 KB	No	1,147 KB	2%	9/30/2012 1:10 AM
Entropy_v5u1	Compressed (zipped) Fol...	1,257 KB	No	1,258 KB	1%	9/30/2012 1:11 AM
Entropy_v5u2	Compressed (zipped) Fol...	5,144 KB	No	5,095 KB	1%	9/30/2012 1:11 AM
Fly Crypter + Uniq Stub Generator.r...	RAR File	657 KB	No	664 KB	1%	1/30/2010 7:03 PM
Fly Crypter v2f.rar	RAR File	478 KB	No	494 KB	4%	11/18/2009 4:51 PM
[redacted]	Compressed (zipped) Fol...	96 KB	No	96 KB	1%	9/30/2012 1:13 AM
Grieve Crypter	Compressed (zipped) Fol...	464 KB	No	465 KB	1%	9/30/2012 1:14 AM
Hacking Crypter.rar	RAR File	72 KB	No	72 KB	1%	12/23/2009 2:00 PM
Heavens Crypter V1	Compressed (zipped) Fol...	220 KB	No	221 KB	1%	9/30/2012 1:15 AM
HHC 1.4.0.rar	RAR File	382 KB	No	381 KB	0%	12/26/2009 1:44 PM
Hidden Sight Crypter	Compressed (zipped) Fol...	2,367 KB	No	2,366 KB	0%	9/30/2012 1:16 AM
icrypt Gold	Compressed (zipped) Fol...	3,744 KB	No	3,753 KB	1%	9/30/2012 1:16 AM
Illusi0n Crypter	Compressed (zipped) Fol...	66 KB	No	66 KB	1%	9/30/2012 1:16 AM
Infinity Crypter 2.rar	RAR File	103 KB	No	104 KB	2%	1/30/2010 7:06 PM
Infinity Crypter.rar	RAR File	215 KB	No	218 KB	2%	1/14/2010 3:29 PM
Insanity Crypter V3.0.0	Compressed (zipped) Fol...	25 KB	No	25 KB	1%	9/30/2012 1:17 AM
Jamaica Crypter.rar	RAR File	232 KB	No	232 KB	1%	12/26/2009 1:44 PM
L3G!T™ Public Crypter 1.1	Compressed (zipped) Fol...	23 KB	No	24 KB	1%	9/30/2012 1:17 AM
Level-23 LuOpP CrYpT v1.2.rar	RAR File	3,981 KB	No	3,984 KB	1%	1/14/2010 3:31 PM
Level-23 LuOpP CrYpT V1.3.rar	RAR File	3,918 KB	No	3,925 KB	1%	1/30/2010 7:07 PM
Li0n Polymorphic Crypter	Compressed (zipped) Fol...	1,056 KB	No	1,063 KB	1%	9/30/2012 1:18 AM
LiQuid Vapour V2.0.rar	RAR File	207 KB	No	208 KB	1%	12/18/2009 12:01 PM
Mingo Crypter V1 Mod By MINGO....	RAR File	86 KB	No	86 KB	1%	12/24/2009 8:53 PM

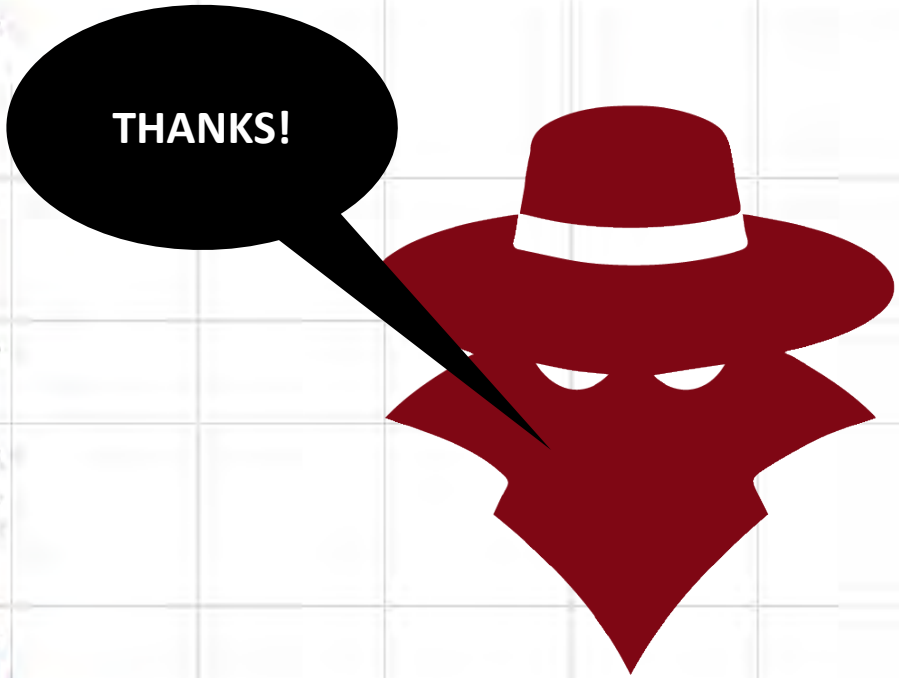
RANSOMWARE KITS ADDED CAPABILITIES



NOT JUST...

REALLY SOPHISTICATED CAPABILITIES

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Service Execution	File System Permissions Weakness	File System Permissions Weakness	Code Signing	Hooking	File and Directory Discovery	Remote Desktop Protocol	Email Collection		Data Compressed	
	Windows Management Instrumentation	Hooking	Hooking	File Deletion		Network Service Scanning					
		Kernel Modules and Extensions	Process Injection	Modify Registry		Process Discovery					
				Process Injection		Query Registry					
				Software Packing		System Network Configuration Discovery					
						System Time Discovery					



WITH BITCOIN INCREASING IN VALUE...

HACKERS KNOW A LOT OF MONEY CAN BE MADE...

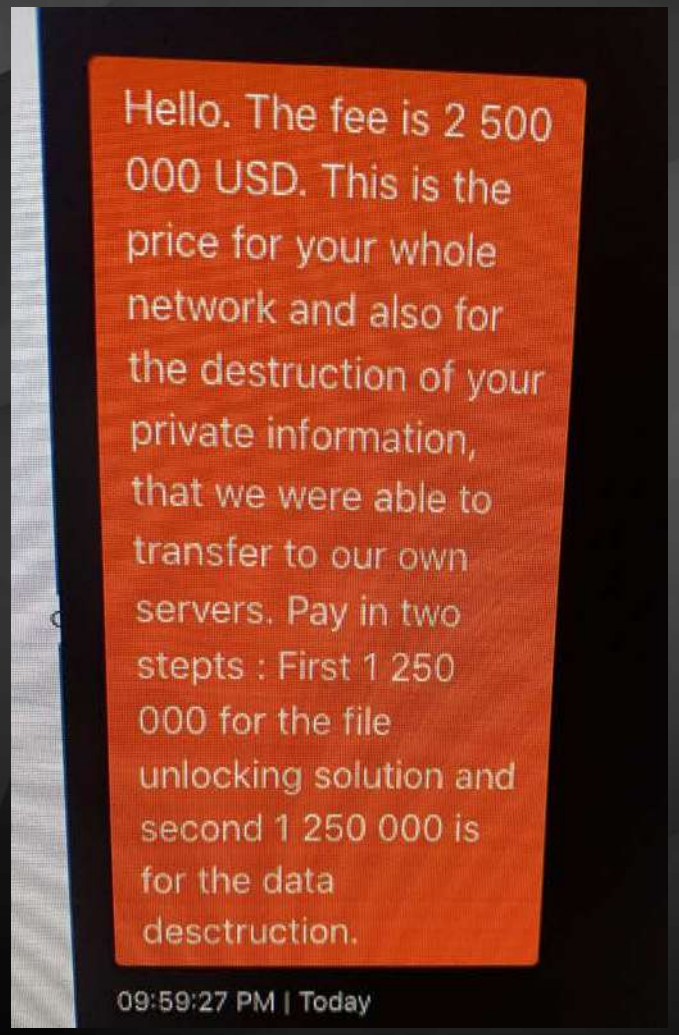
NOW RANSOMING DATA IS THE LAST ACTIVITY...

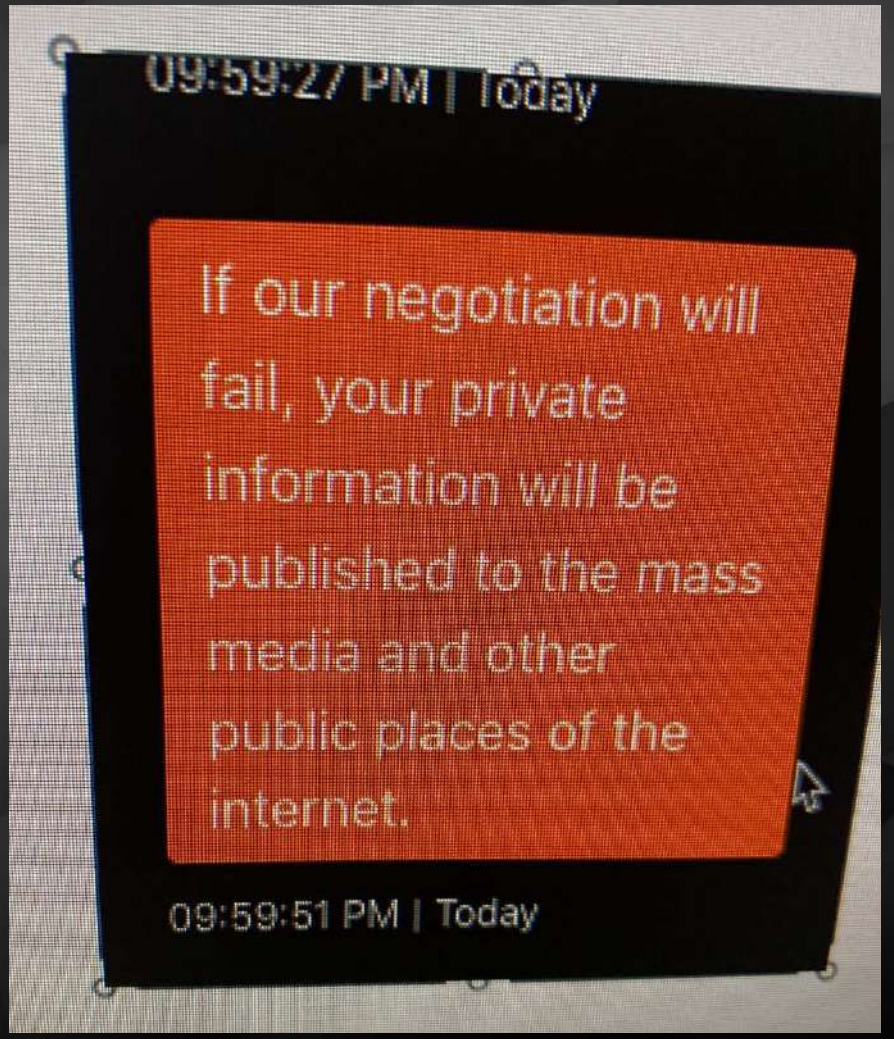
The mean dwell time (time between compromise and detection) was a global average of 146 days

Source- FireEye

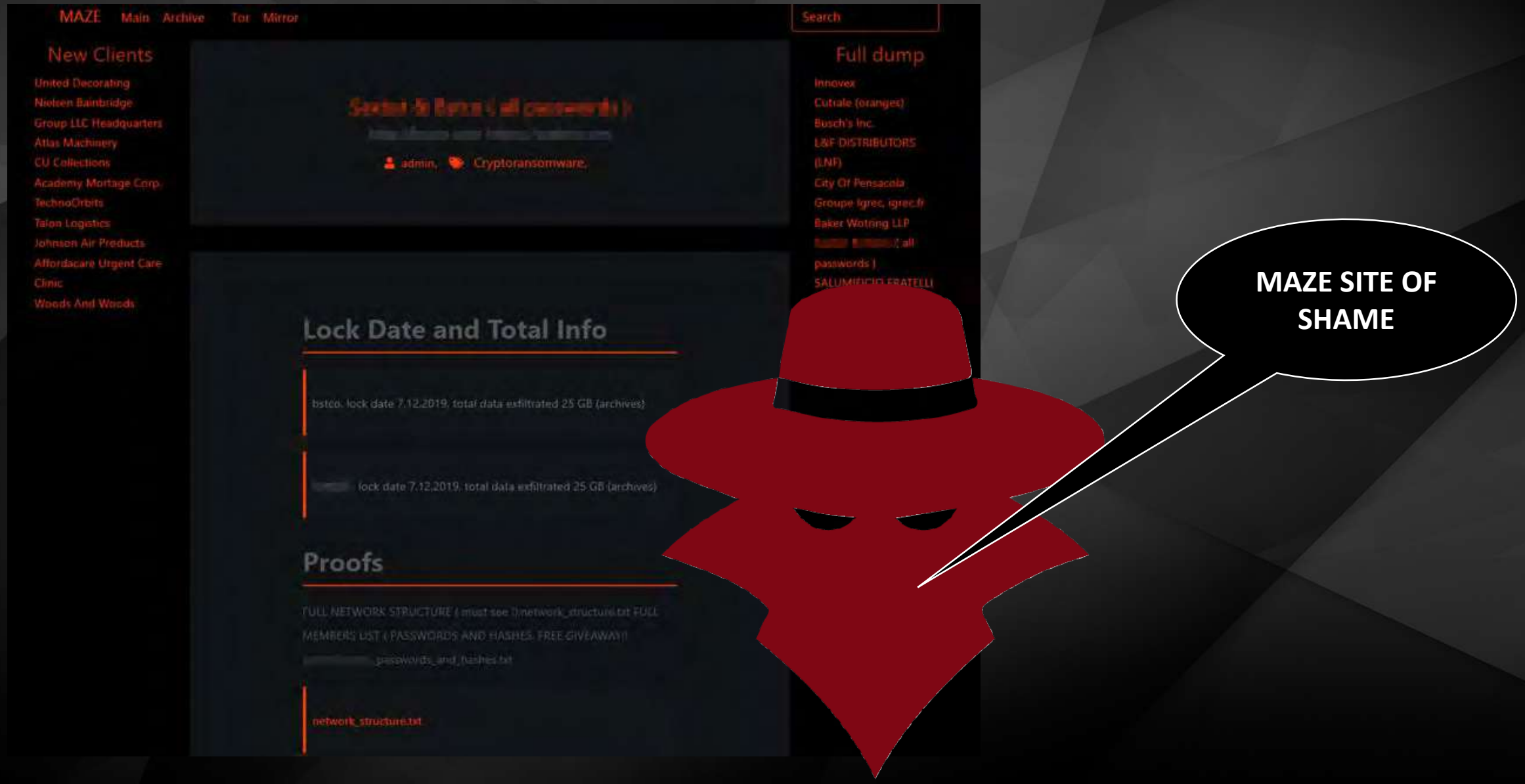
EXFILTRATION OF DATA IS THE MONEY MAKER!!!

RANSOMING THE DESTRUCTION OF DATA STOLEN





PAY UP! OR BE PUBLICALLY SHAMED!



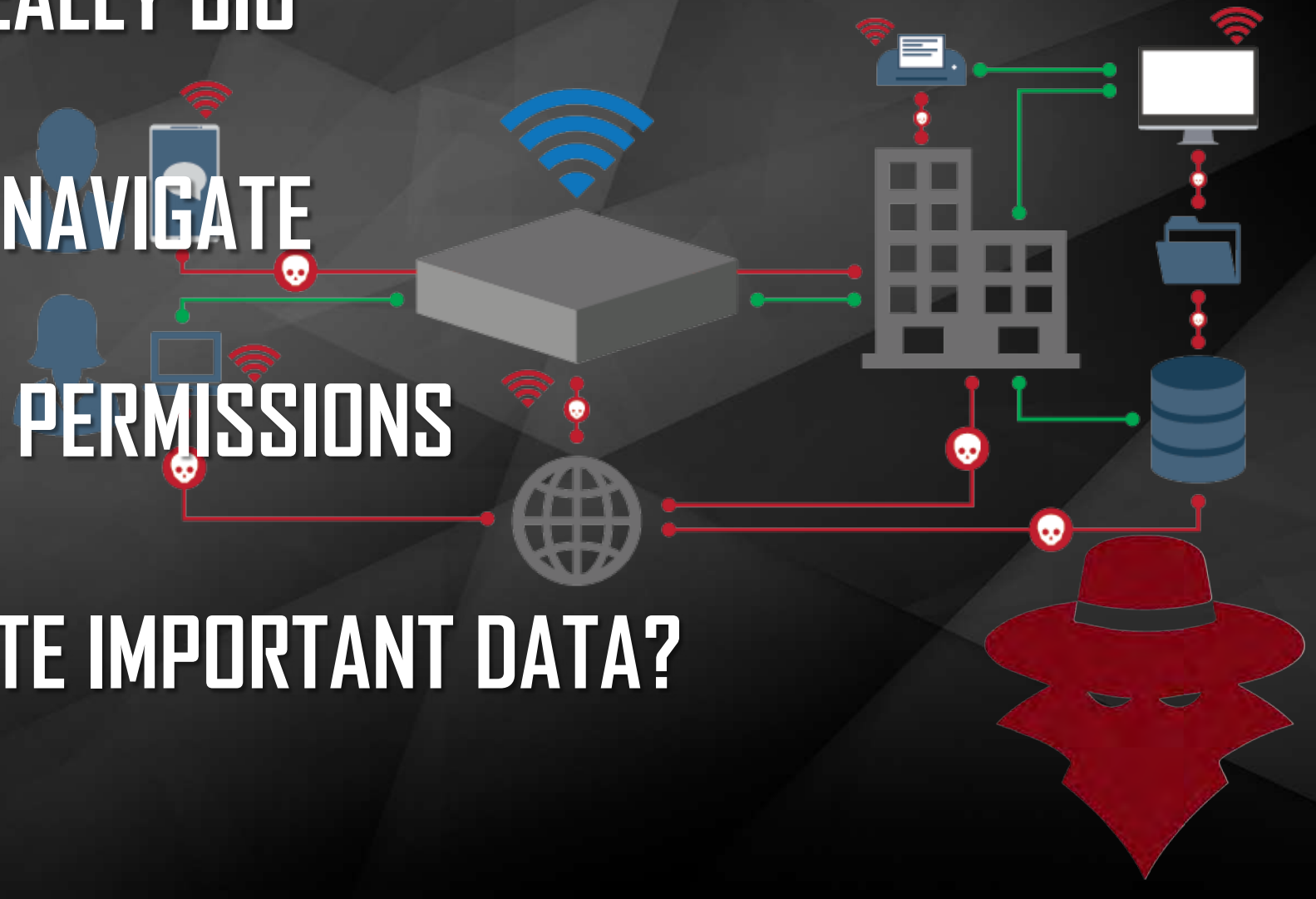
HOW DO HACKERS QUICKLY FIND IMPORTANT DATA?

NETWORKS CAN BE REALLY BIG

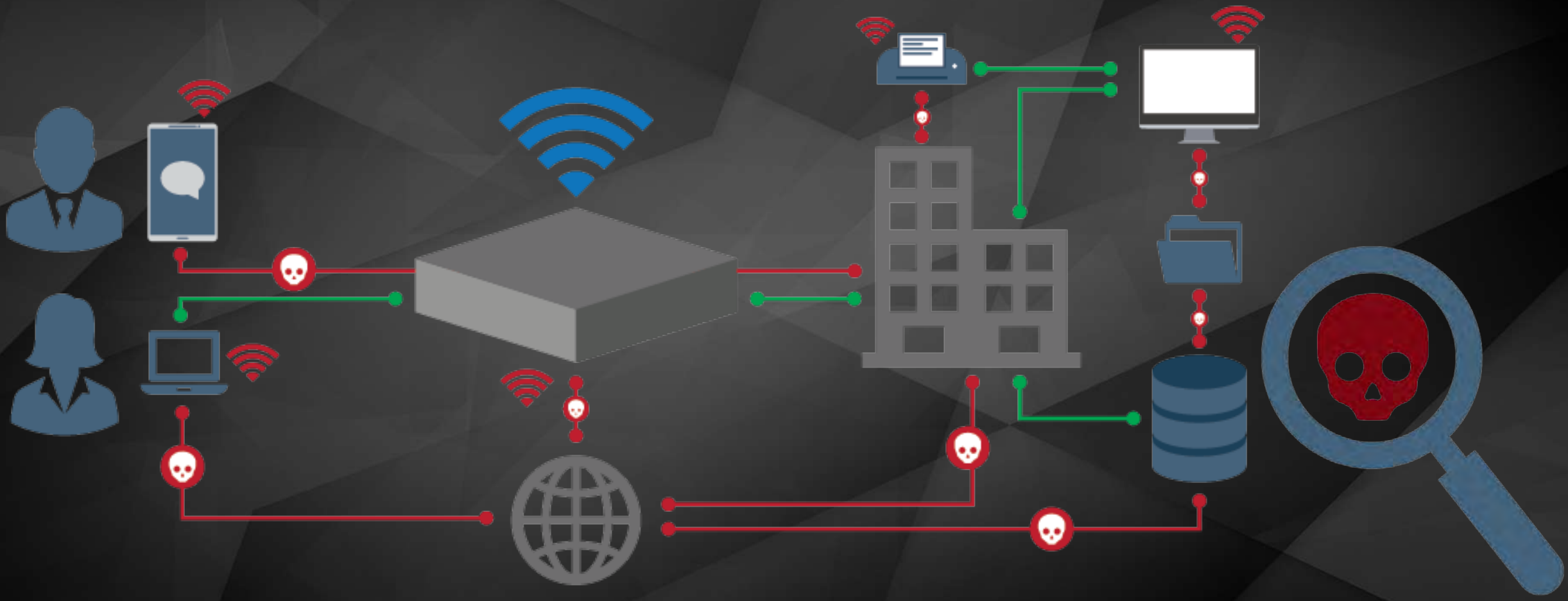
COMPLEX & HARD TO NAVIGATE

HAVE CONTROLS AND PERMISSIONS

HACKERS STILL LOCATE IMPORTANT DATA?



USERS OFTEN ENABLE HACKERS TO FIND THE DATA



USERS OFTEN PROVIDE A ROADMAP

HOW?

USERS OFTEN DO NOT FOLLOW POLICY

THEY PLACE OR MOVE DATA HOWEVER THEY CAN

USING EMAIL TO FIND DATA

FINDING DATA STORES USING EMAIL

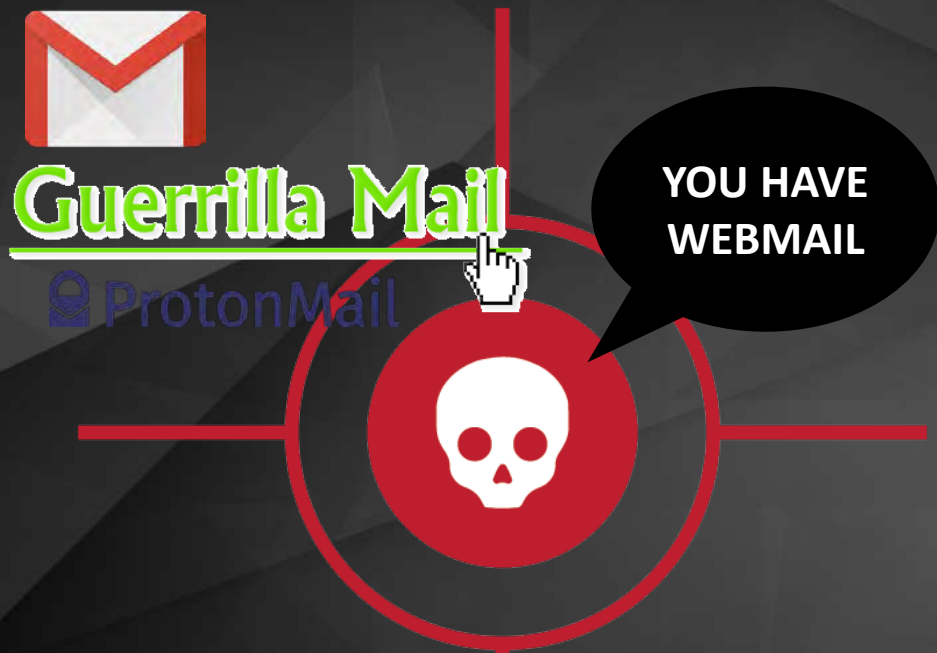
POORLY SECURED EMAIL

POORLY MANAGED EMAIL

MOST INBOX'S ARE FILLED WITH PII

INBOX LEADS TO INTELLIGENCE

FINDING DATA USING WEBMAIL



PRIVATE WEB EMAIL

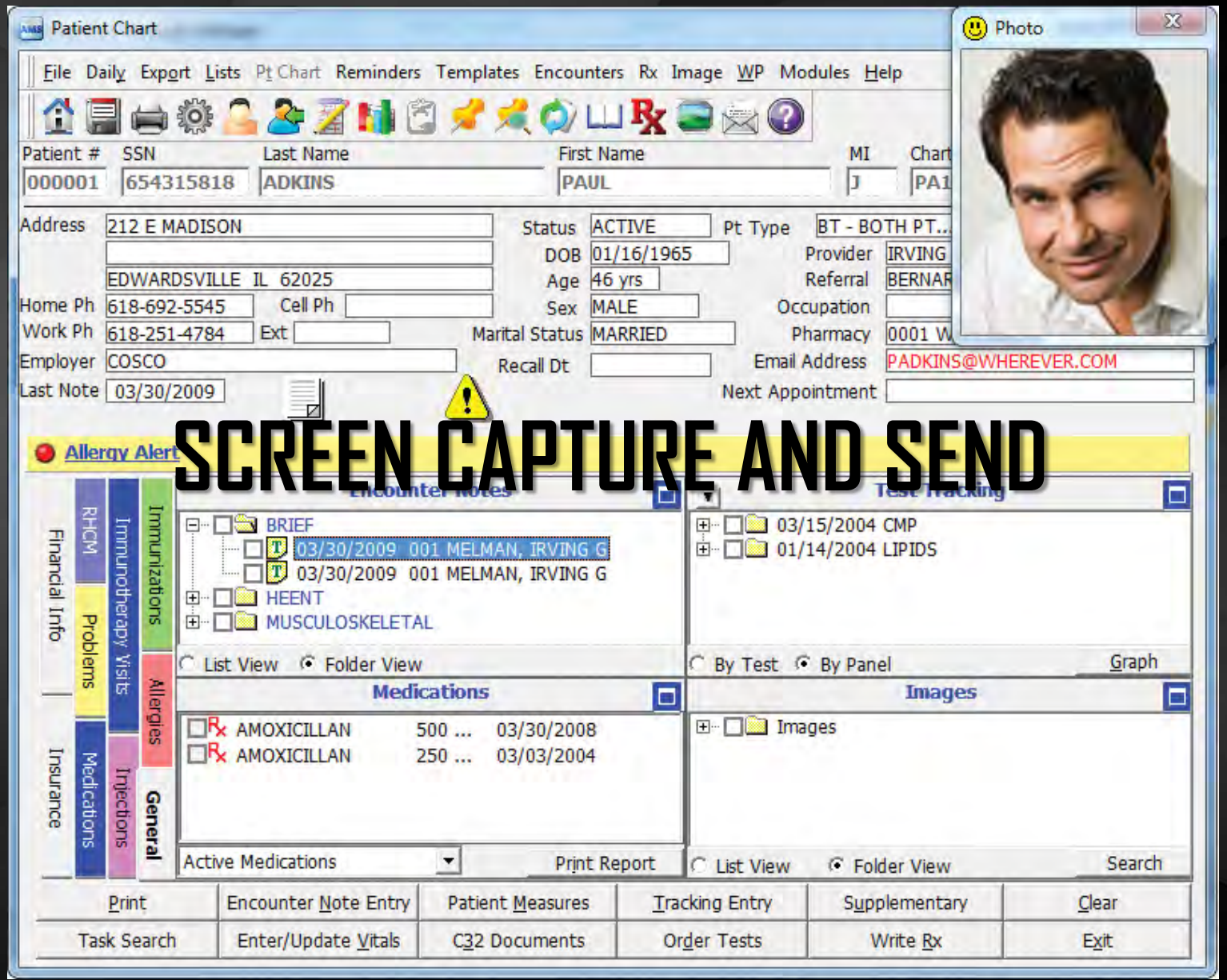
USERS USE TO BYPASS DLP

WILL USE BASED ON FILE SIZE

USERS MAY THINK ITS FASTER

THIS CREATES A DATA LOSS DISASTER

FINDING DATA STORES USING EMAIL



FINDING DATA STORES

FINDING DATA STORES ON A NETWORK

SYSTEMS

INBOX INSTRUCTIONS? WHATS THAT?

SYSTEM RESETS

SYSTEM TRAINING

SYSTEM DOCUMENTATION

FINDING DATA STORES – WEB SERVICES

WEB SERVICES

LEVERAGE COMPROMISED SYSTEMS

LOOK THROUGH THE "FAVORITES"

LOOK THROUGH THE HISTORY OF THE USERS

MOVING STUFF THROUGH A POORLY PROTECTED RESOURCE

FINDING DATA STORES-SHARES

SHARE

LOOK FOR A SHARED FOLDER

USED AS A METHOD OF CONVENIENCE

MOST TIME NO CONTROLS

STUFFED FULL OF THINGS WE SHOULDN'T SEE

DATALOSS CASE STUDY

HOW A SHARE CAN CRIPPLE YOU

FINDING DATA STORES – USB STUFF

USB STUFF

LOOK FOR ANYTHING CONNECTED

BACKUPS ARE OFTEN TIED TO USB HD DRIVES

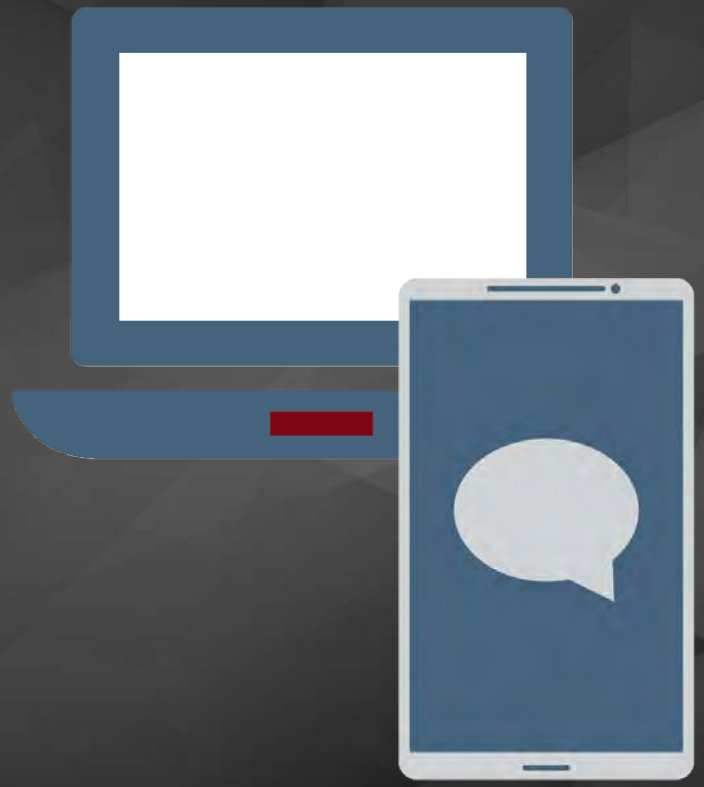
USB HAS LIMITED CONTROLS

OFTEN FILLED WITH STUFF DEEMED "IMPORTANT"

DATALOSS CASE STUDY

HUMAN RESOURCES DISATER VIA

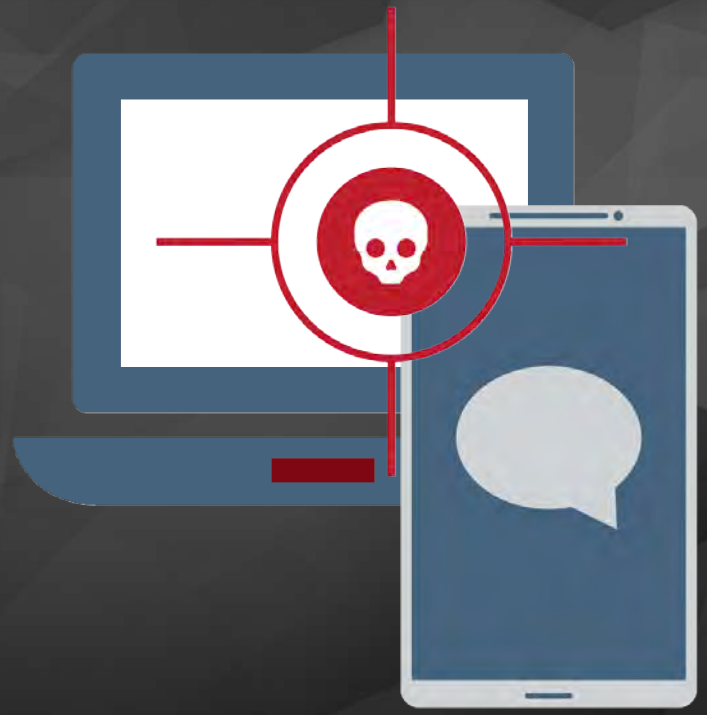
FINDING PHYSICALLY LOST DATA



NO ENCRYPTION LEADS TO BIG TROUBLE

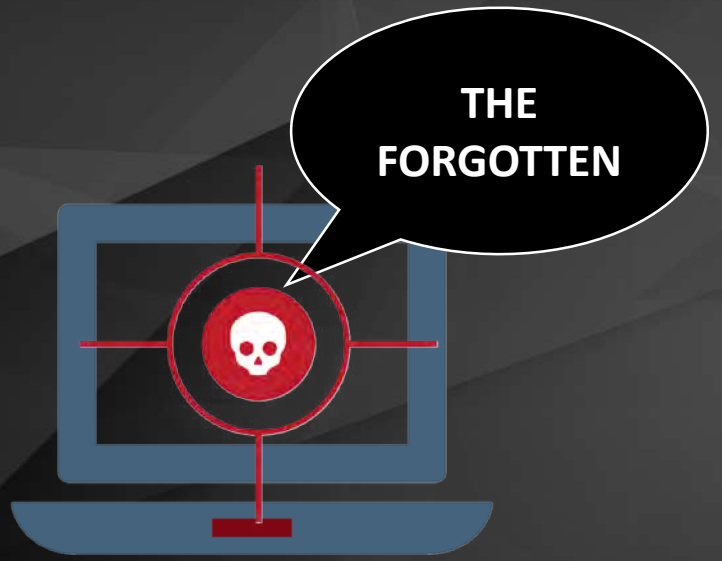
DATALOSS CASE STUDY

LOST HARDWARE CREATES A DISASTER



FINDING BIG DATA STORES

FINDING DATA STORES – LEGACY SYSTEMS



OLD FAX SYSTEMS ARE A PERFECT START

SYSTEMS WITH OLD OPERATING SYSTEMS

OLD SYSTEMS OFTEN HAVE POOR AUTHENTICATION

DECOMMISSIONED BUT NEVER REMOVED

COMPROMISE A SYSTEM TO GET DATA?

SYSTEMS

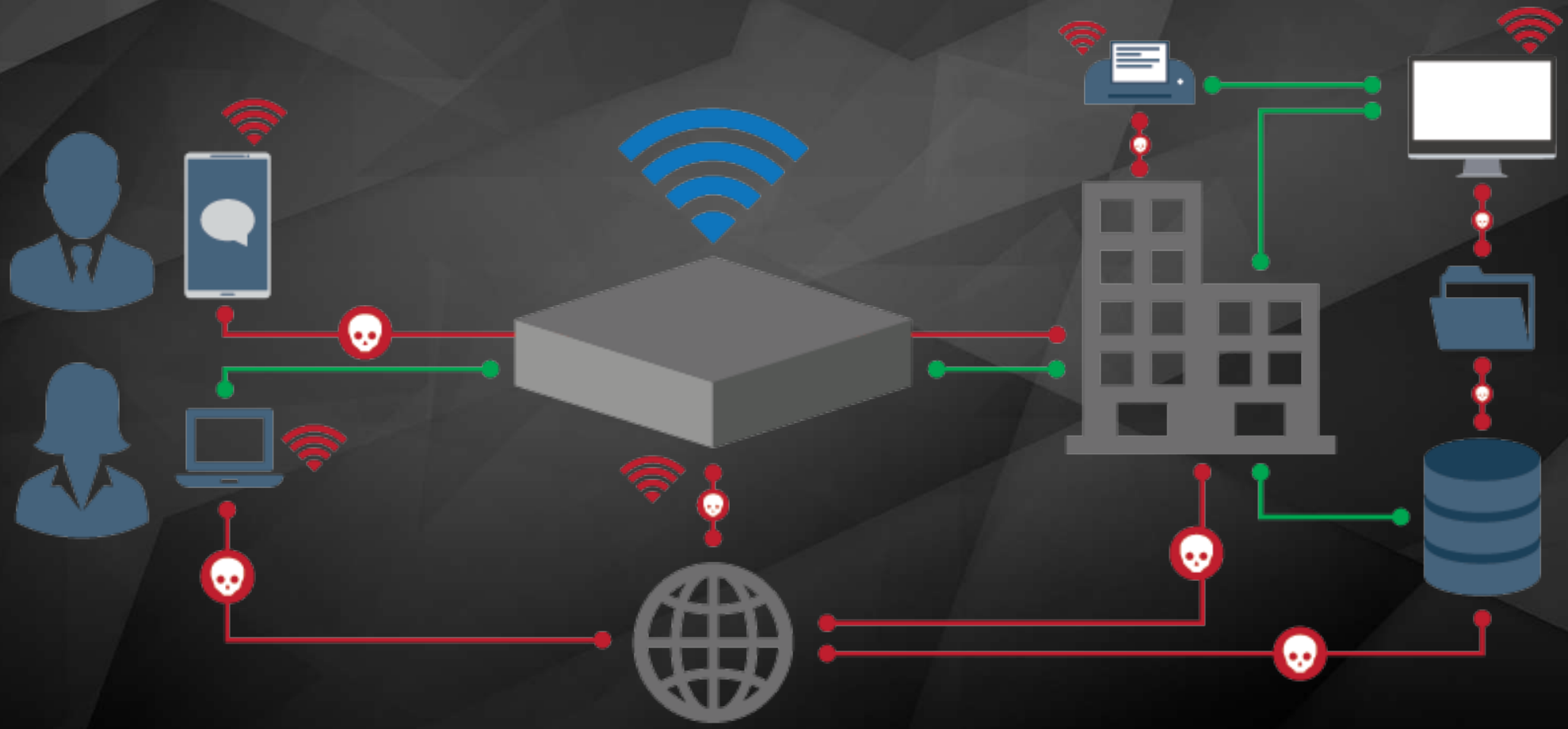
GET MORE NETWORK PRIVILIDGES

SCAN NETWORK FOR A VULNERABLE SYSTEM

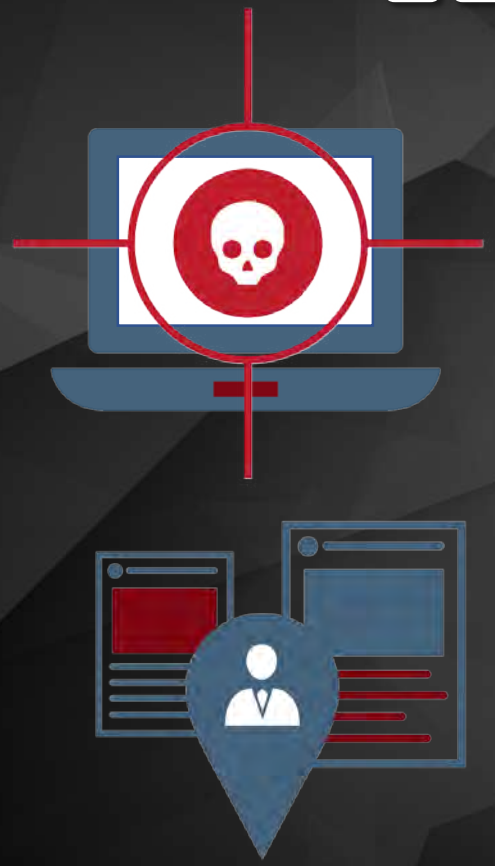
EXPLOIT THE VULNERABLE SYSTEM

GO FROM USER TO ADMIN TO DOMAIN ADMIN

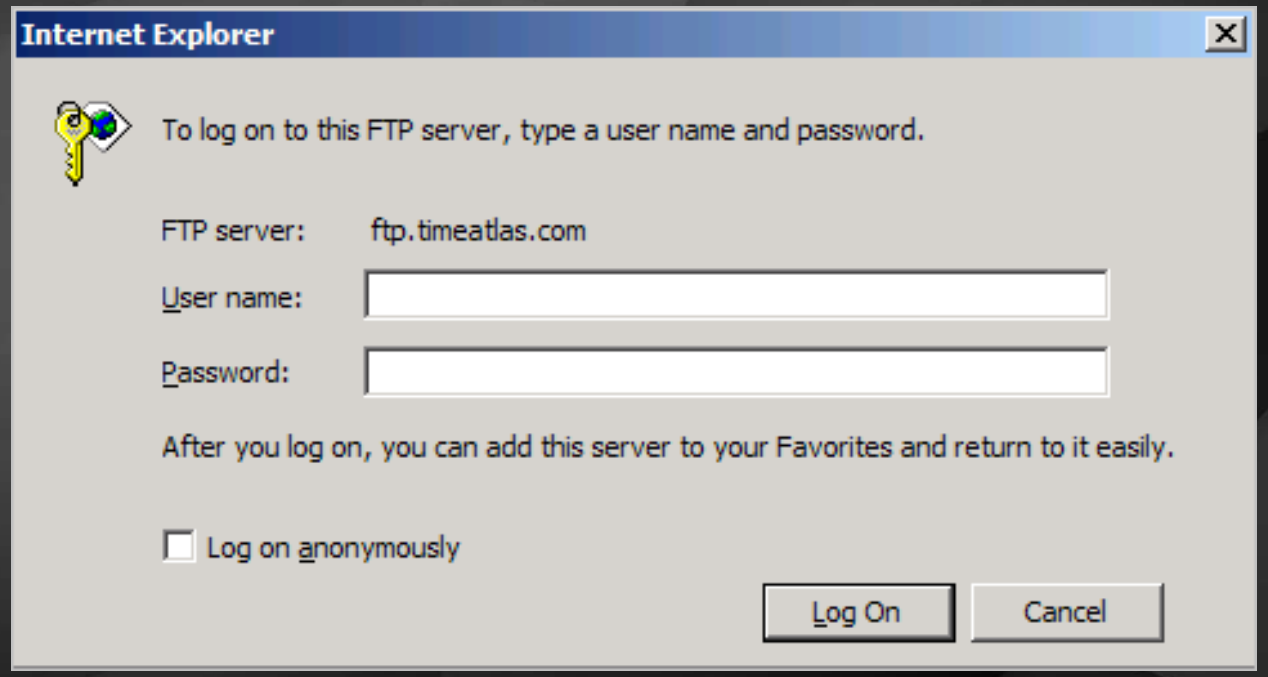
DATA BECOMES INCREASINGLY VISIBLE



USING NETWORK SERVICES TO MOVE DATA?

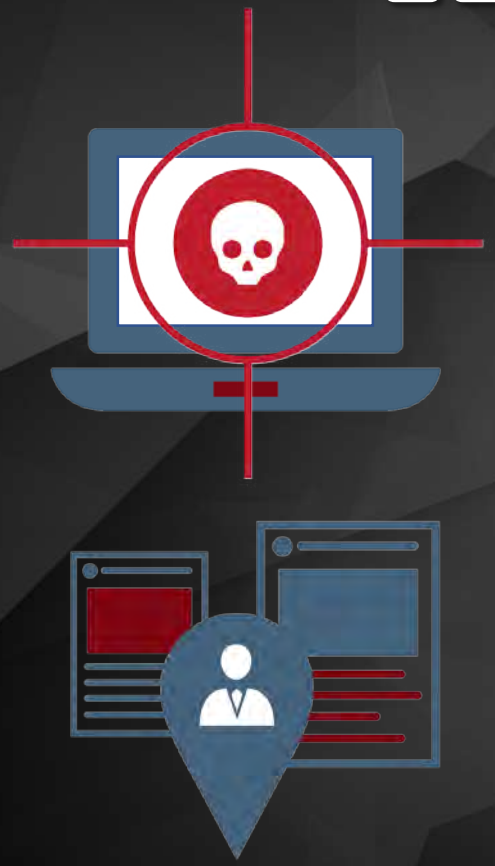


UNNECESSARY OPEN FIREWALL PORTS



FTP (Port 21)

USING NETWORK SERVICES TO MOVE DATA?



UNNECESSARY OPEN FIREWALL PORTS

RDP (Port 3389)

DATA IN THE CLOUD

ON SITE RESOUCES

CO-LOCATED RESOURCES

CLOUD SERVICE MODELS

SOFTWARE AS A SERVICE (SaaS)

PLATFORM AS A SERVICE (PaaS)

INFRASTRUCTURE AS A SERVICE (IaaS)

YOUR JUST MOVING DATA TO ANOTHER PLACE

CLOUD DATA SECURITY ISSUES

IaaS/PaaS CONCERNS

DON'T MAKE THE ASSUMPTION YOUR DATA IS SAFE

TAKE PRECAUTIONS TO HARDEN SECURITY OF YOUR CONTENT

SECURITY RECOMENDATIONS...

- TRAIN USERS TO FOLLOW POLICY
- IF POSSIBLE, IMPLEMENT A DATA LOSS PROTECTION SYSTEM
- EXAMINE SYSTEMS AND NETWORK FOR SENSITIVE DATA

SECURITY RECOMENDATIONS...

- LEVERAGE ENCRYPTION AS MUCH AS POSSIBLE
- HARDEN CREDENTIALS TO DATA STORES
- IMPLEMENT TWO FACTOR IF POSSIBLE

SECURITY RECOMENDATIONS...

REVIEW VENDOR APPLICATION FOR SECURITY CONTROLS

ASK FOR THE LAST SECURITY TESTING RESULTS

DON'T MAKE THE ASSUMPTION YOUR DATA IS SAFE IN THEIR POSSESION

QUESTIONS?

CONTACT US:

Steve Stasiukonis
Managing Partner – Secure Network Technologies
315.579.3373
steve@securenetworkinc.com

William N. Wildridge III
CEO/Managing Partner - Microscope
315.430.6838
wwildridge@microscopeHC.com