ATLANTIC DATA FORENSICS

In Data There is Truth™

Current State of Hacker Attacks

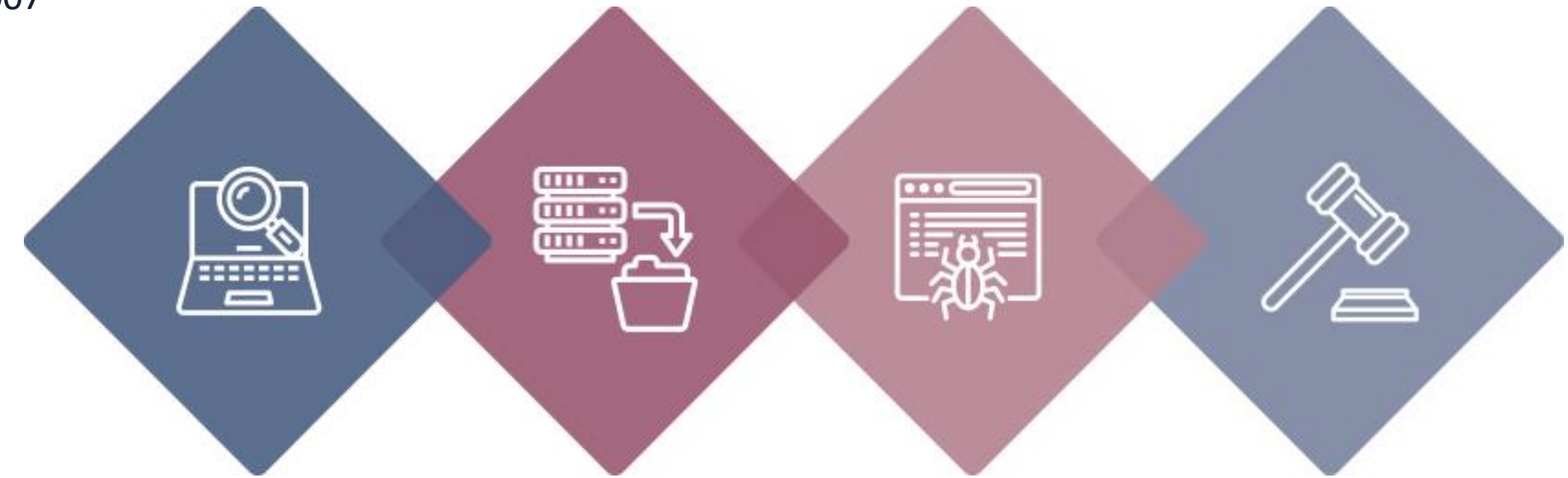
NMTC

March 2021

Presented by
Brian Dykstra

Reactive Investigation Services

SINCE 2007



Computer Forensics

Determining which user stole the customer list, when that photo was taken, who deleted data, and more.

E-Discovery

Helping attorneys get to relevant data quickly and efficiently, and helping companies understand their data landscape.

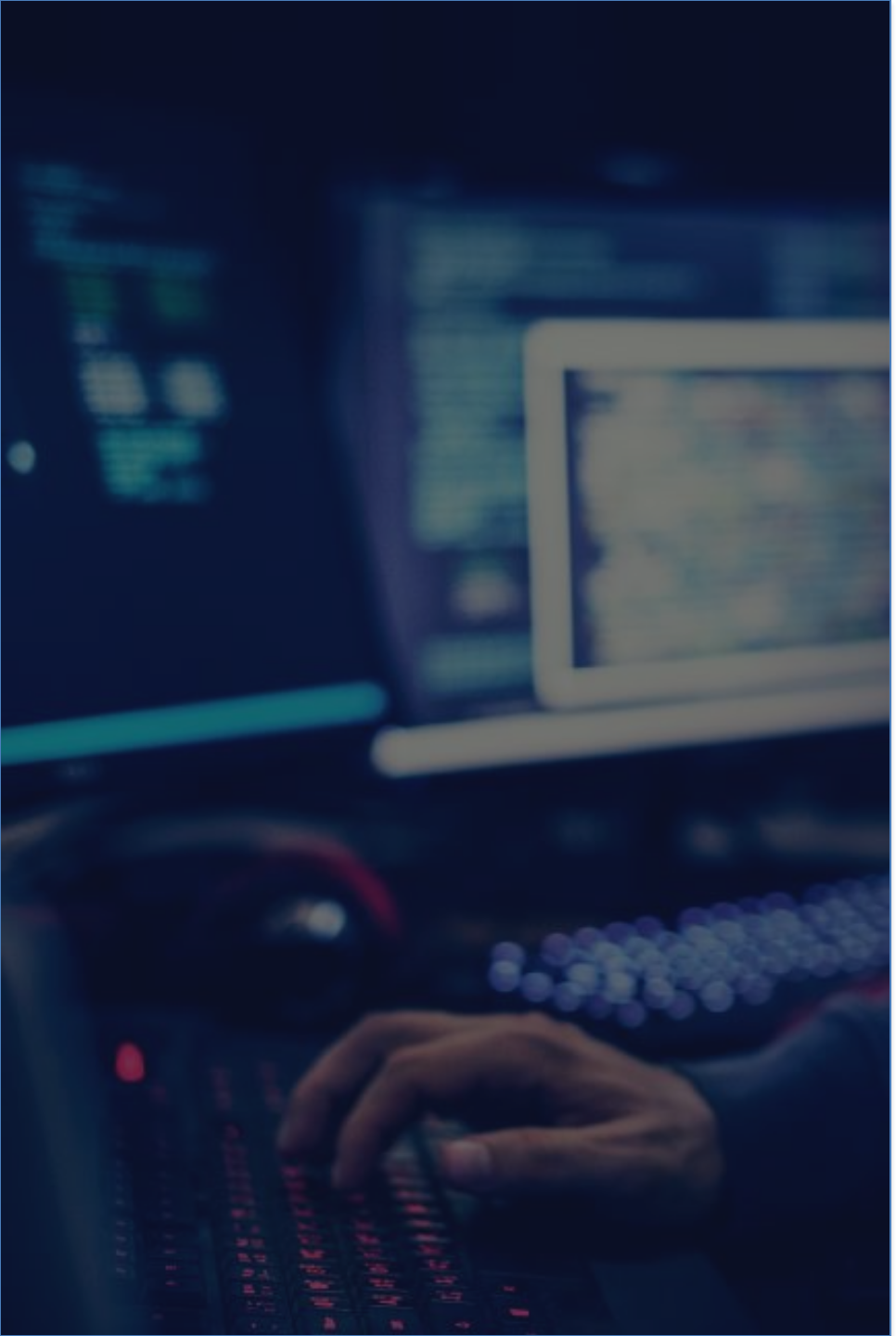
Incident Response

Removing hackers, insiders, malware, and ransomware from enterprise networks.

Expert Witness Testimony

We advise on digital evidence strategy, and firmly stand behind everything we do in hearings, depositions, and at trial.

ATLANTIC DATA FORENSICS



The Internet vs Business

- Remote Access Exploitation
- Ransomware
- ACH Fraud
- 3 Magic Security Solutions
- Process Not Product

ATLANTIC
DATA FORENSICS

Remote Access Exploitation

- Citrix ADC
- Pulse Secure VPN
- F5 BIG-IP
- FortiGate SSL-VPN
- Microsoft RDP
- Palo Alto Global Protect SSL VPN
- NordVPN
- SonicWall SSL VPN
- MobileIron Mobile Device Management (MDM)

ATLANTIC DATA FORENSICS

What We Saw In 2020-2021

- January-February – Lot's of access to networks via Citrix ADC and Citrix ADCs being taken over to mine Bitcoin
- March-July – APT group attacks on companies based upon exploitation of Pulse Secure VPNs and F5 BIG-IP traffic aggregators
- August-December – Attacks from groups abusing SSL VPN flaws from FortiNet, Palo Alto and SonicWall
- Microsoft RDP exposed to the Internet is a hacker gift that keeps on giving
- The year finished out with a slew of SolarWinds Orion exploits
  - This one still isn't over
- Yesterday's Exchange Server vulnerability by Volexity is going to be huge

ATLANTIC DATA FORENSICS

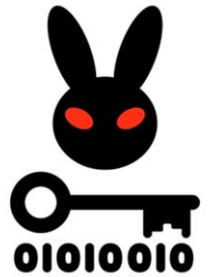
Ransomware

- The average cost of a ransomware attack on businesses was $33,000. (Source: Sophos) ADF numbers $100,000+
- 60% of small businesses hit by ransomware go out of business within the year (Source: AIG) ADF – It definitely happens
- Ransomware attacks have increased over 97 percent in the past two years. (Source: Phishme)
- 34% of businesses hit with malware took a week or more to regain access to their data. (Source: Kaspersky) ADF – Typically 30 days or more
- Ransomware payouts are becoming more expensive (Million$)

ATLANTIC DATA FORENSICS

Ransomware to Extortionware

- Since before the second half of 2019 we've seen a change in the way ransomware groups are working
- Ransomware is no longer about a user clicking on a link or something in their email
- Ransomware is now generally a symptom of a larger data breach
- Hackers are stealing sensitive corporate data an demanding a ransom or they will publish the data



ATLANTIC DATA FORENSICS

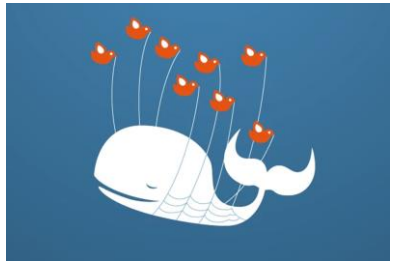
Increasing Sophistication

- Ransomware As A Service (RaaS) is now a thing
- The Maze ransomware group recently announce that they had formed a cartel with LockBit to publish victim data
- REvil (Sodinokibi) is auctioning victim data and doing a NASDAQ notification; Nefilim is releasing victim data; Netwalker runs a blog; Conti researches targets
- The quality of techniques used by ransomware is improving with process and memory injection, antivirus shutdown and log wiping

ATLANTIC DATA FORENSICS

Just A Management Failure

- Ransomware is a failure of management at multiple points and on multiple levels:
  - CEO/CFO – Staffing and budget failure
  - COO – Requiring outdated or legacy systems be continued
  - CIO – Network structure and data backup failure
  - CISO – Patch management and endpoint security



ATLANTIC DATA FORENSICS

ACH Fraud Phishing

- ACH Fraud Phishing involves no malware or hacking
- It is especially dangerous to small businesses because they typically have no email security configured
- ACH Fraud Phishing schemes usually involve breaking into a CFO or finance related mailbox and doing no harm
- The fraudster then emails a number of the company's clients and asks them to send payments to a new bank
- More sophisticated versions of ACH Fraud Phishing involves “mimic” domain names and even fake phone numbers

ATLANTIC DATA FORENSICS

How to Lose $8M Through BEC

- Phisher compromises a CFO at Company A
- Phisher then uses Company A's CFO's email account to phish a bunch of other CFOs
- Once the phisher has a collection of CFOs the fraud starts
- By examining the CFOs' email content they determine who clients are and what average invoices look like
- The phisher then send change of ACH payment instructions and waits for or sends out new invoice
- Typically these sort of BEC attacks aren't recognize for more than 60 days

ATLANTIC DATA FORENSICS

The 3 Magic Things

Based upon Incident Response support to hundreds of organizations in a wide variety of industries, small & large

- Good perimeter control
- 2FA/MFA
- Antivirus/Anti-Malware

ATLANTIC DATA FORENSICS

GOOD PERIMETER CONTOL – FIREWALLS & VPNS

- Your firewall has to actually be doing its job – Blocking & Logging
- Turn on GEO-IP filtering
- Turn on Anti-virus/Anti-malware protections
- Block all the vendor recommended services (RDP, SMB, etc.)
- Whitelist sites that servers or critical systems can reach
- Ensure that logs from your firewall get stored
- Don’t just log what is rejected by the firewall
- Have someone periodically review the dashboard
- Don’t forget about Cloud firewalls

ATLANTIC DATA FORENSICS

2FA/MFA

- It works if you apply it to everything
- At a minimum apply 2FA to Administrator accounts
- Apply MFA to all your Office 365 & Gmail users
- Don’t accept the idea of a “user revolt”
- Ensure that your logs actually show you who logged in and from where
- Extend your 2FA to Cloud solutions using SAML
- Stops a lot of BEC/Account compromise/Phishing

ATLANTIC DATA FORENSICS

ANTIVIRUS/ANTI-MALWARE

- It’s not sexy but it will work a lot of the time
- AV must be installed on everything to full protect an organization
  - Laptops and desktops
  - Servers
  - Email
  - Firewalls
  - Cloud
- Don’t skip the Macs; They get lots of viruses
- For added protection go to an MDR solution

ATLANTIC DATA FORENSICS

TECHNICALLY – 4 THINGS

- Operating systems and applications patches
- They are free from vendors, so we don’t include them in the 3
- Applying vendor patches to operating systems and common applications (Adobe, QuickBooks, Chrome, Zoom, Citrix)
- Don’t forget about patching core IT infrastructure
  - Firewalls
  - VPNs
  - Citrix ADC
  - Cameras
  - Phone systems

ATLANTIC DATA FORENSICS

Security is a Process Not a Product

- #1 Security Threat – Not enough IT staff or unqualified IT staff
- Lots of companies look to MSPs, Lots of MSPs are bad at their jobs
- 2FA is free (or cheap) and easy
- Patching operating system is free and easy
- Anti-virus/Anti-malware is cheap and easy – MDR/EDR is great
- Cloud back-up is cheap and easy – 3 tier backups
- Logging computer activity is cheap and easy – A few extra hard drives and a PowerShell script
- Encryption is free and easy – Save yourself from a lost laptop problem

ATLANTIC DATA FORENSICS

ATLANTIC DATA FORENSICS

In Data There is Truth™

THANK YOU

7310 Esquire Court, Suite 5B • Elkridge, Maryland 21075

www.atlanticdf.com

contact@atlanticdf.com or direct brian.dykstra@atlanticdf.com

410-540-9000

For 24/7 Incident Response call 1-800-270-9034