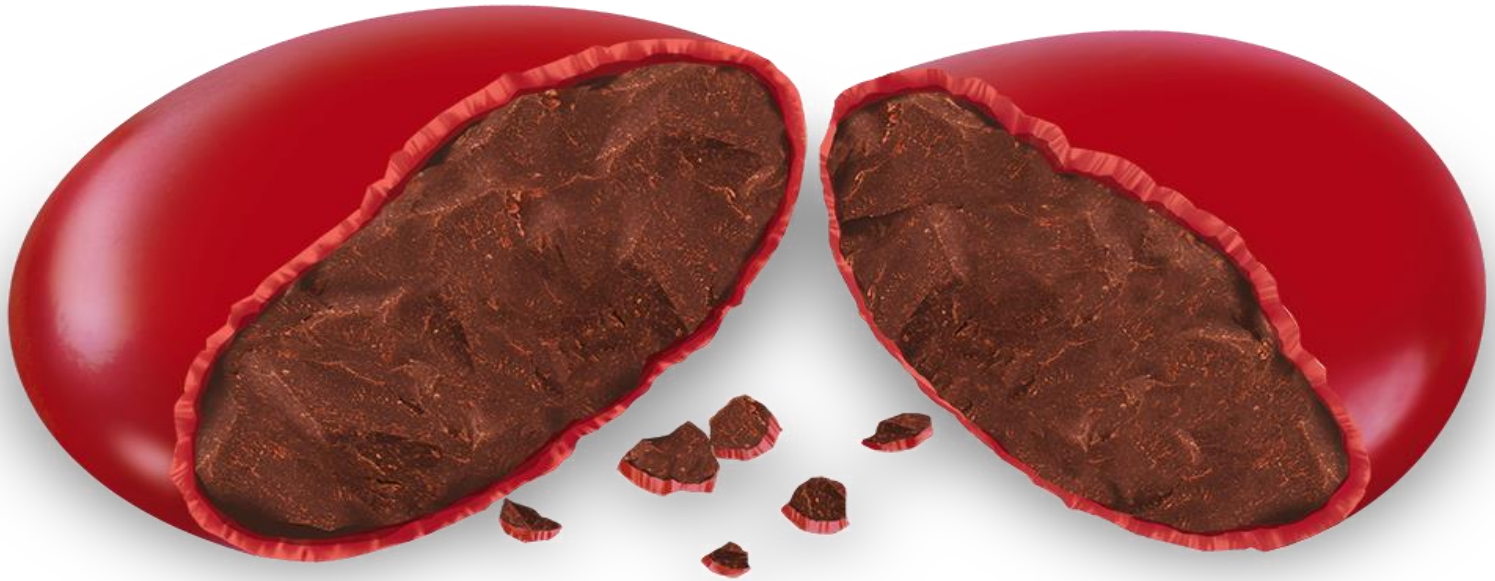
ExtraHop

Ransomware: Hard to Stop for Enterprises, Highly Profitable for Criminals

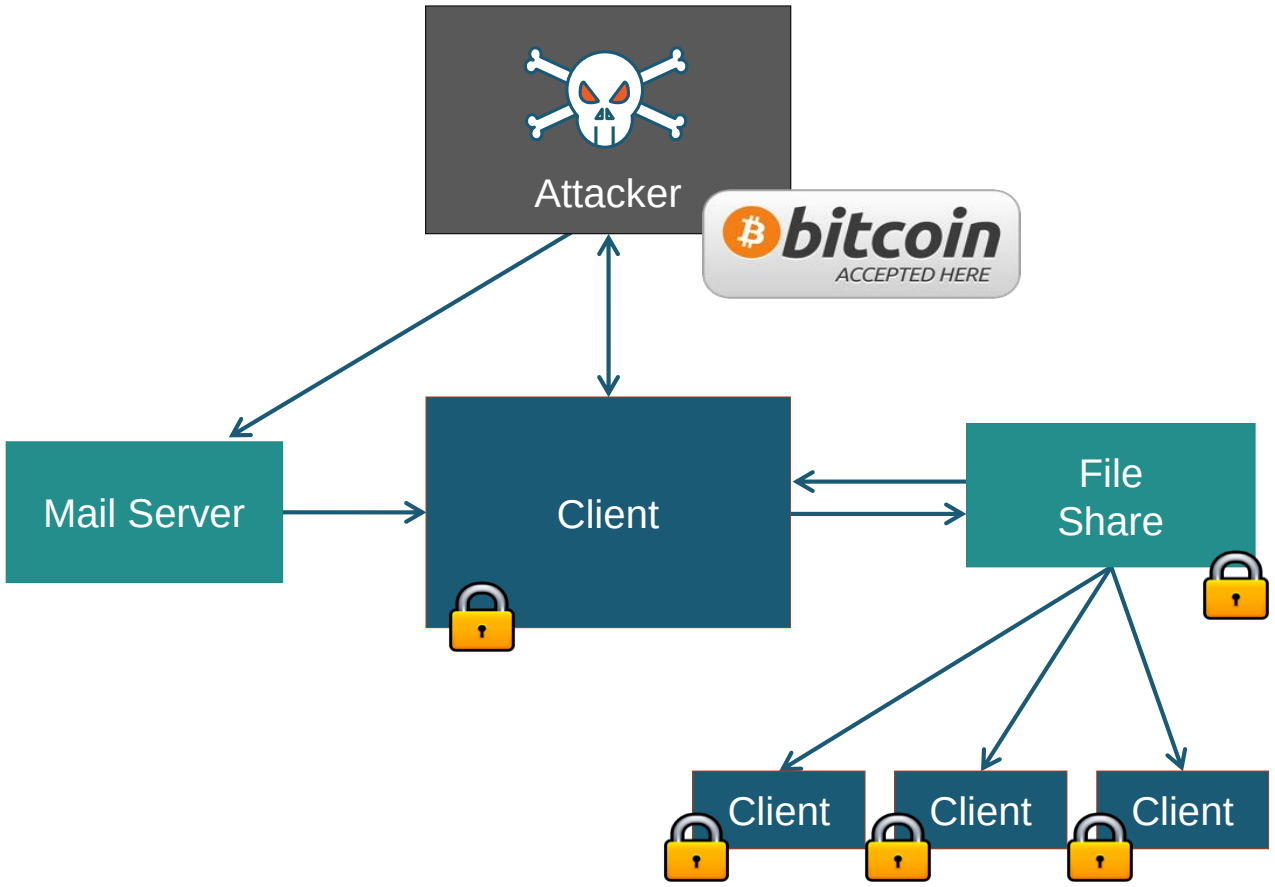
Peter Connolly, SE

Adrian Turner, EMEA Partner Manager

The Problem: An M&M Security Model



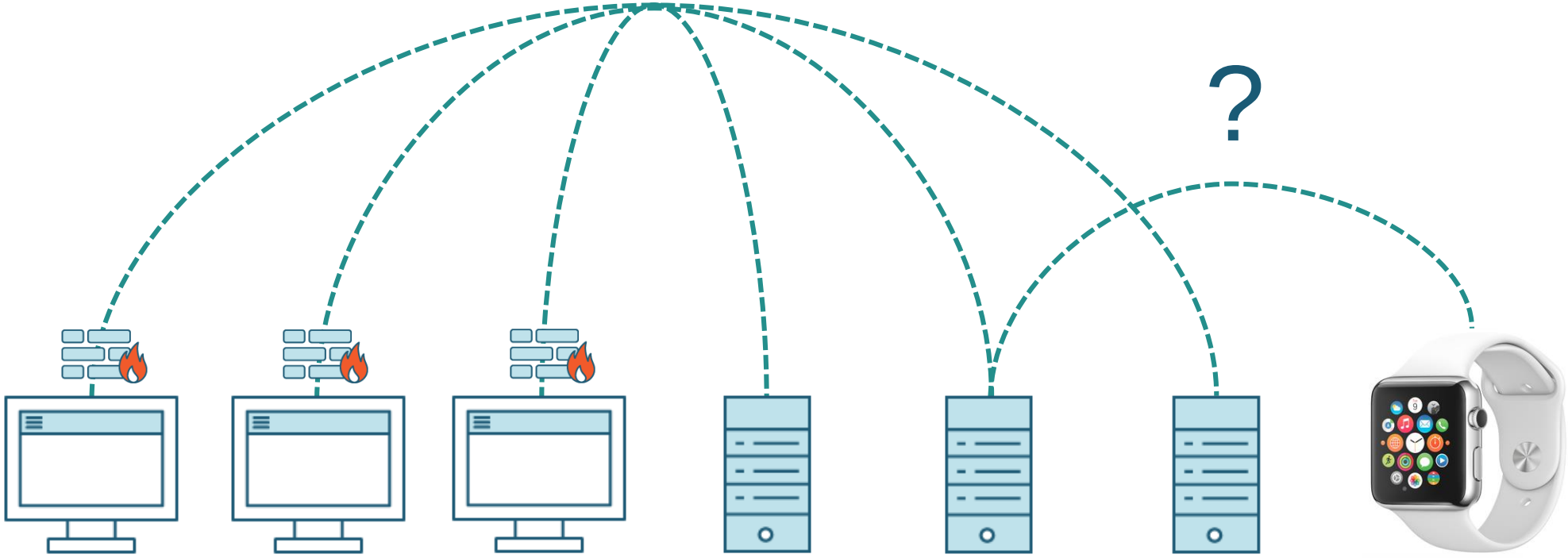
Ransomware: Easy Money for Criminals



1. A user's machine gets **infected with malware**
2. The malware **downloads an encryption program**
3. Begins **encrypting files on the client**
4. **Spreads to network shares** that the client is connected to
5. **Spreads infected document(s)** to other users/systems
6. **Ransom is paid using Bitcoin**, which is extremely difficult to track

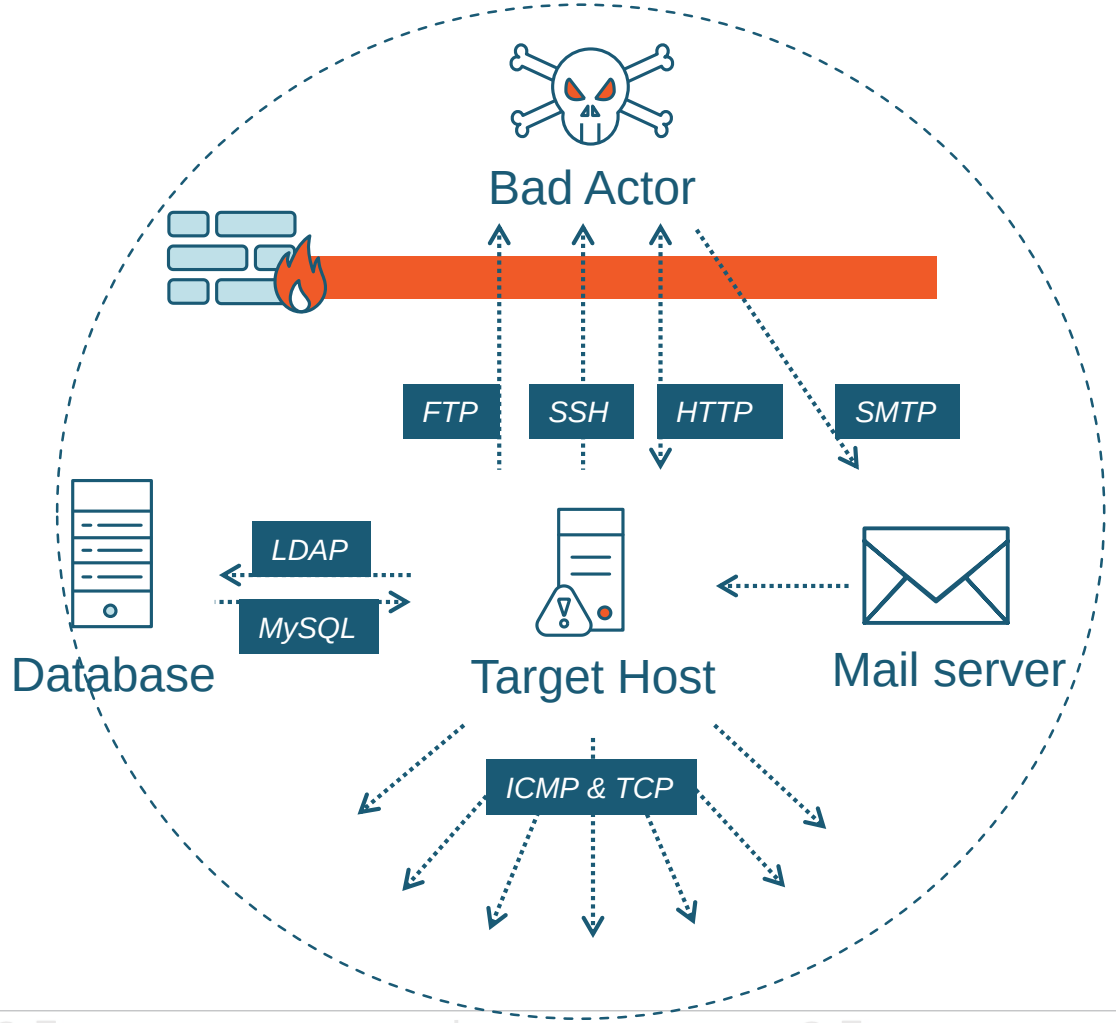
Rogue Devices with Credentials

Agent-Based Firewall



Everything Transacts on the Network

… even the bad guys



- Various behaviors
- Data exchanged across boundaries (north-south, east-west)
- Takes place slowly, over a period of 30+ days

Comprehensive observation has never been possible until now

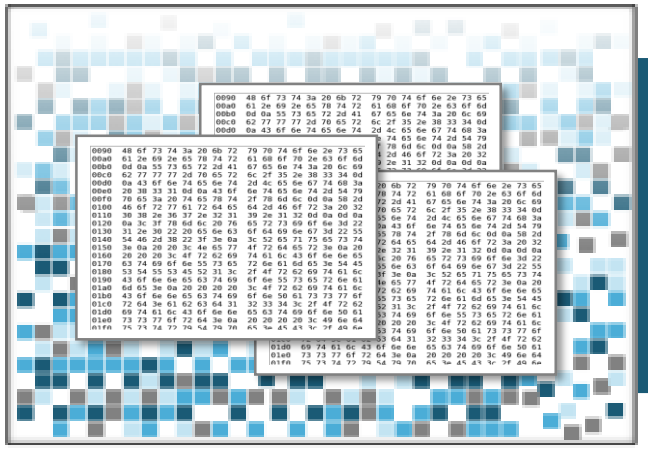
Analyze Data in Flight to Understand Risk

- What clients are affected?
- Which files and shares?
- Where is the malware from?
- Where else should I look?
- Can I spot this in the future?

Most importantly … catch ransomware attacks *live*, in real time

Wire Data = Risk Visibility

Unstructured Packets



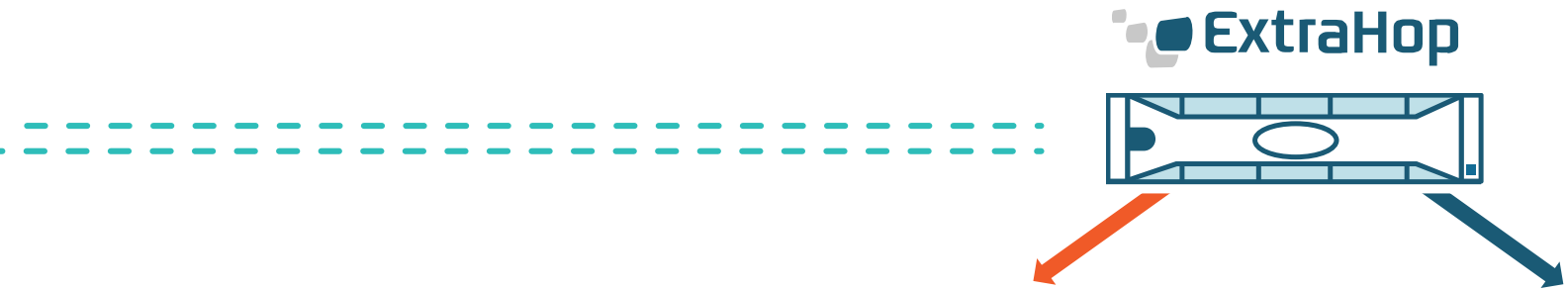
Stream Analytics

Structured Wire Data

Application & User Behavior	Protocol Activity	Encryption Profile	Compliance	CVE Detection
Privileged user logins	Unencrypted FTP	Certificate expiration	SSH tunneling	Shellshock
Unauthorized connections	Telnet	Key length	Non-standard ICMP	HTTP.sys
Lateral network traversal	Gopher	Outdated SSL sessions	Non-standard DNS	Turla malware
Brute force attacks	TACACS	MD5/SHA-1 cert signing	Non-standard HTTP	Heartbleed
Storage/DB access	SNMP v1, v2, v2c	SSL traffic by port	Disallowed file types	FREAK SSL/TLS
Fraudulent transactions	Finger	Email encryption	Invalid file extension writes	POODLE
Large data transfers	IRC	Wild card certificates	Blacklisted traffic	Logjam

Add Wire Data to Your Existing Infrastructure

Integrate with your existing security tools to make them smarter



Automate intelligent firewall actions

Quarantine ransomware-infected clients

Supplement threat intelligence

Verify policy enforcement

Check Point SOFTWARE TECHNOLOGIES LTD. · WatchGuard · paloalto NETWORKS · FireEye · DELL SonicWALL

Enrich SIEM platforms

Improve detection of threats inside the perimeter

Trace historical activity leading up to an event

Store user login activity

sumologic · Radar · ArcSight An HP Company · splunk> · LogRhythm · Big Data lake for security

Real-World ExtraHop Use Cases

Proactively Assess Actual Risk Profile	
Application Behavior & Anomaly Detection (ABAD)	• Database and HTTP response sizes vs baseline • Queries used in SQL injection attacks • Protocols used on non-standard ports • Citrix ICA launches that are “out of profile”
Network Behavior & Anomaly Detection (NBAD)	• Traffic for banned ports and protocols • Compromised servers connecting to Russian domains via DNS • Massive DDoS using UDP:80 traffic • Detect lateral movement via scanning/probing
Business Process (Layer 7) Anomaly Detection	• Phishing scams and bot/screen scraper detection • Attempted fraud activity • Unexpected HTTP methods/content types
Attack Surface Reduction	• Compromised servers within the corporate network • Insecure ciphers and key sizes
Security Infrastructure Monitoring / Control Validation	• Firewall rules testing/validation • Network segregation (e.g. QA/Prod) • Security scans/testing that may disrupt operations • Proxies, blocking technologies are blocking things inappropriately • Locked-down VDI environment validation

How Customers Use ExtraHop Today

A platform for a range of InfoSec use cases

"We generate huge amounts of data, but prior to ExtraHop, we had no scalable way to mine that data, let alone extract insight and value from it. With ExtraHop, we can now gain a really good understanding of the **who, what, when, where, and how** of our environment."

- Lee Riches, Operational Analyst, Sportingbet

sportingbet

Application Behavior & Anomaly Detection (ABAD)
Network Behavior & Anomaly Detection (NBAD)
Business Process (Layer 7) Anomaly Detection
Attack Surface Reduction
Security Infrastructure Monitoring / Control Validation

Network and Application Forensics
Data Exfiltration Detection
Realization of Threat Intelligence
Availability

Compliance
Authentication Monitoring
Encryption and Certificate Analysis

Demo